NISTIR 7314

Building Tactical Information System for Public Safety Officials

Intelligent Building Response (iBR)

David G. Holmberg
William D. Davis
Stephen J. Treado
Kent A. Reed

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NISTIR 7314

Building Tactical Information System for Public Safety Officials

Intelligent Building Response (iBR)

David G. Holmberg
Stephen J. Treado
Kent A. Reed
Building Environment Division

William D. Davis
Fire Research Division

U.S DEPARTMENT OF COMMERCE
National Institute of Standard and Technology
Building and Fire Research Laboratory
Gaithersburg, MD 20899-8600

January, 2006

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary
TECHNOLOGY ADMINISTRATION
Michelle O'Neill, Acting Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William A. Jeffrey, Director

Abstract

The Building Tactical Information project begins the process of developing technology and standards to realize the vision of making real-time building information accessible to emergency responders to enable safer and more efficient emergency response. This project addresses both the information needs of the fire, police and emergency medical services and the technology needed for moving building data out to emergency responders. A workshop was held to gather information on first responders' building information needs, and presentation standards have been examined based on emergency responder needs while enroute to an incident and on-scene. A technology data path is proposed that will allow information collection and transport to the emergency responder. A security analysis addresses the security concerns of the information transfer. A demonstration of the technology, with a decision support system transmitting real-time building information to first responders, was held at NIST and forms the basis for a documentary video.

Executive Summary

The vision for the Building Tactical Information project is to provide more and better information to emergency responders in order to make building incident response safer and more efficient. The challenge is to develop a standard method for collecting, moving and displaying information to those who need it, so that all important building information is available to emergency responders when they need it.

The main goals of the project were to: (i) gather information about what information first responders need; (ii) develop a standard path for moving data from buildings to first responders; (iii) demonstrate the proposed technology with a video to document the demonstration; and (iv) address security concerns of the information transfer.

For the first goal, a workshop was held in May 2004 and a report of gathered information was published (Jones et al., 2005). A summary of this information ("Workshop White Paper") is also included in Appendix A of this report. Those results have already been incorporated into proposed presentation standards, and also used by manufacturers of systems to display information to first responders. Section 2 of this report gives a brief summary of the workshop.

A method for collecting and moving data from a building to the public safety network has been developed, and this technology path is presented in this report. Section 3 discusses the building information server, decision support tools that process data, and also reviews work done on presenting data to first responders in an understandable format. That work on presentation has been submitted to NEMA (National Electrical Manufacturers Association) for consideration in their standards development process.

A demonstration of the technology was held at NIST in February, 2005, and a documentary video of the demonstration was produced. It was recognized that first responders do not generally know what information is available from building control systems, and so an additional educational video has been produced. The demonstration is summarized in Section 3.4. The videos are available online and on CD.

A security analysis is presented in Section 4, and in conjunction with the efforts of the US Department of Homeland Security SAFECOM program is under continuing development as an architecture for a standard public safety network. Section 5 reviews relevant standards development work, and Section 6 presents overall conclusions.

This work has been supported by the National Institute of Justice (NIJ) via the Community Oriented Policing Services (COPS) office and administered through the NIST Office of Law Enforcement Standards (OLES).

Table of Contents

1 Introduction

Providing public safety officials, including emergency responders, with critical information from building automation systems can help them make better tactical decisions for a safer and more efficient response. Fundamental to accomplishing this is a standard means of collecting and transporting building information (and most importantly real-time system data) available in buildings out to the public safety officials that need it. This includes providing information to fire and police responders, emergency medical responders, emergency dispatch centers, city and state governments, national guard, criminal investigation units, and others who might need the information at the time of a building incident or afterwards. A standard for collecting and moving data enables interoperability of products made by different companies and can make the technology more available to public safety departments.

There are two underlying visions that drive this work. First is creating a building knowledge database at the design phase of a building that is then carried into the operation phase of the building life-cycle, with information about the building that is available to outside partners. Second is developing the means for emergency responders to access real-time building information from building systems in a useable format.

The foundation of this work is thus a combination of these two visions—that there should be a standard means of collecting and transporting building information out to the emergency responders and public safety officials who need it. This report presents the efforts of the Building and Fire Research Labroatory (BFRL) to move a step closer to this reality.

1.1 Intelligent Building Response

Today's modern buildings function with multiple control systems programmed to run different building systems, such as heating ventilation air-conditioning (HVAC), lighting, access control (physical security), and life safety (fire). Network communications carry commands from controllers to actuators and switches, and a host of sensors feed data back to controllers. Yet, for the most part, all this information is bottled up in the building even while it could provide tremendous situational awareness to those outside the building, telling them where a fire is, where smoke is, where occupants are, which devices are operating, which lights are on, or which doors are open.

Why should first responders need to do a size up at the scene in order to find out what is happening inside? Real time information regarding building systems should be available while they are enroute to the scene. Why can't a dispatcher understand the emergency inside the building from the start of an incident, even before the apparatus is dispatched? Lacking now is a standard method of moving real-time building data out of the building into the hands of emergency responders.

A modern building fire system has fire sensors in every room to report alarms when the smoke level or temperature reaches a set threshold. These same fire signals might be processed by a computer to identify growth and progress of a fire. That information could be passed to firefighters before they arrive on scene. In addition to fire sensors, the HVAC system might provide temperature data. The lighting system could identify rooms with lights on where occupants could be located. The elevator system could report elevator location, as well as presence of smoke and/or high temperatures. And the access control system could identify forced entry as well as provide video feeds from cameras.

Today, most large commercial buildings, and many industrial and special-use buildings, have building automation systems (BAS) with digital control and each subsystem with a master controller. These systems could be tied together. And while many buildings, especially smaller ones, don't have sophisticated controls, the good news is that those with the greatest number of occupants are the ones with the greatest potential for supplying information about an incident to those responding to an incident.

The current work addresses the challenge of identifying the building information an emergency responder might need and getting it to the people who need it in a format they can understand and use. There are a growing number of smart buildings with sensor data that would be useful to emergency responders, but there is as yet no standard way of collecting that data and presenting it to emergency responders. In order for this to work effectively, there must be an agreed-upon standard that allows: any building equipment manufacturer adhering to the standard to offer data to be collected; a standard building server that can collect that data and offer it up in a standard interface to the public safety network; standard messages for communicating the data; and standard interfaces for public safety end users to see the data.

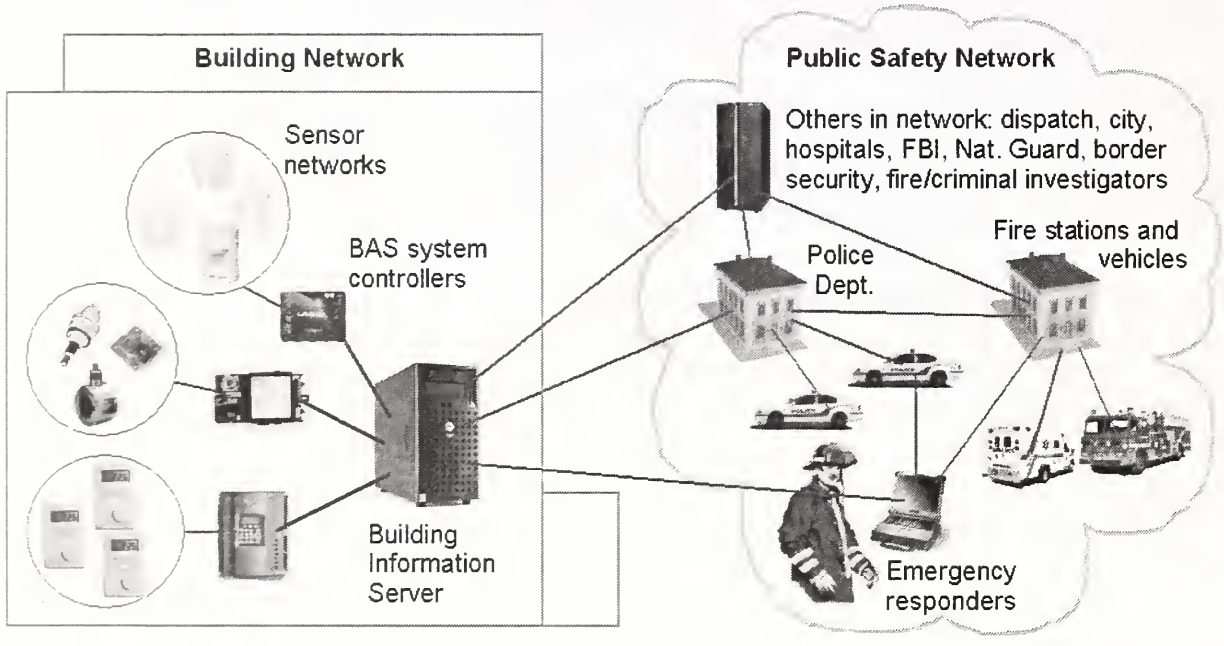


Figure 1 Schematic of system architecture showing data path from building sensors to sub-system controllers to building information server and then to public safety network where it is accessible by public safety officers.

1.2 Background

The NIST Building and Fire Research Laboratory (BFRL) has been active in building communications and information research for many years. In the 1980s NIST helped spearhead the development of what has become the leading building automation protocol, which allows different building control systems to communicate and share information. This standard protocol, called BACnet (Building Automation Control Networks, www.BACnet.org), has been in use for 10 years and is rapidly expanding and being implemented all over the globe. NIST researchers have also been instrumental in addressing the life cycle of building information and how it can be stored, formatted, maintained, and re-used over time. Beginning in the 1980s, NIST has been active in the development of information representation and exchange protocols for the building industry. This work has culminated in the Industry Foundation Classes (IFC), maintained by the

International Alliance for Interoperability (IAI, www.iai-international.org). The IFC establish a common information model that enables information sharing and interoperability throughout all phases of the building life cycle. Major building design system vendors have implemented support for IFC in their products as have developers of many downstream applications such as structural engineering, HVAC design, thermal analysis, code checking, quantity take-off, cost estimation and others.

The work covered in this report was performed for the Office of Law Enforcement Standards (OLES) at NIST as part of a larger NIST-wide effort "focused on identifying and then satisfying the functional/operational telecommunication interoperability and information sharing requirements of the Public Safety community." NIST funding came from the Department of Justice, via their Community Oriented Policing Services (COPS) office.

While the major direction of the project has remained fixed over the course of the work, the plans and organization of the federal government's interoperable communications efforts have seen ongoing change. The Department of Homeland Security, formed in 2002, has taken on the role of addressing communications interoperability for emergency response. The Office of Management and Budget (OMB) established the SAFECOM program as a high priority E-Gov initiative. SAFECOM now functions as an umbrella program for communications interoperability within the Federal Government, managed by the Department of Homeland Security's Science and Technology Directorate. The mission of SAFECOM is to enable public safety nationwide (across local, tribal, state, and federal organizations) by improving public safety response through more effective and efficient interoperable communications.

Prior to and continuing into the initial part of this project, SAFECOM was working with first responders to get their input on what they wanted in terms of information and public safety network functionality. This resulted in a document titled "Statement of Requirements for Public Safety Wireless Communications & Interoperability, v1.0", released April 2004 (published by SAFECOM, available at www.safecomprogram.gov). This Statement of Requirements (SoR) sets down what the emergency responders want, but fails to include useful real-time building sensor data, and the only building information that is mentioned is that which first responders already have access to in paper format, such as floor plans with fire system component icons.. SAFECOM is now focused on developing a system architecture (that is, the information technology elements) that can enable the interoperable communications envisioned in the SoR. SAFECOM has funded the Institute for Telecommunication Sciences (ITS, the research and engineering branch of the National Telecommunications and Information Administration, NTIA), to develop the system architecture.

1.3 Project Objectives

The current work has as its focus the dual goals of understanding what information first responders need from a building, and then developing a technology path for collecting and moving the data out of a building and presenting to first responders. There were three deliverables:

1. A workshop report summarizing information requirements;
2. Proposed building information standards, which cover the path from building information definition to collection, transmission, and presentation of that information;
3. A video documenting a demonstration of the proposed technology.

Other objectives of the project included: security analysis of the information transfer from building to public safety officer; meeting with key public safety organizations to better understand needs, and interacting with standards bodies to establish standards development efforts; and development of decision support tools and visualization techniques.

A workshop was held in May 2004 and a report of the information gathered was published. Prior to the workshop a white paper was prepared that outlined what building information BFRL thought would be useful to emergency responders based on preliminary meetings and queries. The focus of the workshop was on examining, understanding, and updating the information listed in the white paper. All the details of the workshop are presented in the workshop report [Jones et al., 2005]. Additional contacts with the public safety community are summarized in this report and include ongoing interaction to evaluate the technology under development as part of this project as well as cooperation in producing the project video. The documentary video is available on the project website [http://www.bfrl.nist.gov/ibr/].

The second deliverable includes a number of separate work items. The major ones include work on: information representation (encoding and organization); publish-subscribe technology application to the task of moving data from building to first responder; security requirements for this data collection and transmission; use of computer modeling (decision support tools) to process the building information and make it useful for first responders; and presentation of the information in a useful format.

The output from the workshop has already been incorporated into proposed presentation standards, and also used by manufacturers of systems to display information to first responders. The security analysis is presented in this report, and is under continuing development in conjunction with the efforts of SAFECOM to develop an architecture for a standard public safety network. A technology path has been outlined for how to collect and move data from a building to the public safety network. That technology path is presented in this report. A demonstration of that technology was held at NIST in February 2005, and a documentary video produced.

In addition to the documentary video, a second video was needed. In the course of various interactions with first responder groups, it became clear that these responders did not understand the information available in modern buildings. As we explained to them what information could be made available, the concept of "intelligent building response" became more clear and the potential for improving emergency response obvious. We also recognized that not all users and equipment vendors and political figures recognize the need for standards, but that communicating this is important.

Therefore, as a means to communicate the potential of utilizing building information in emergency incident response, and the importance of standards, the second video was produced. This video has been released on CD and is also available on the project website [http://www.bfrl.nist.gov/ibr/]. This video seeks to invite all participants in the standards creation process to join in the effort of making building information available to emergency responders.

2 Workshop on Building Information for First Responders

On May 3, 2004, the National Institute of Standards and Technology (NIST) conducted a workshop on information needs for first responders. The purpose of this workshop was to meet with the community of first responders who are responsible for public safety with the focus on use of data contained in building systems. The main issue was identifying what building information would be of benefit to emergency responders at different stages of response to a building emergency and how it should be conveyed. The workshop included representatives from the police, fire, medical, building technology, government, and security communities.

To set the stage for the workshop, NIST prepared a draft white paper on the issues of specific building information needed by emergency services. The information contained in the draft white paper was based on material from National Fire Protection Association committee 1620 ("Recommended Practice in Pre-Incident Planning"), pre-fire plan information from publications (online and print) and fire departments, and discussions with individual local first responders. Information was also used from a meeting of chief officers of fire and police to discuss the need and potential use of building information in emergency response, held in July 2003 at NIST.

The approach of this workshop was to bring together speakers from different public safety organizations (fire, police, building technology, government, and security/terrorism) and to have attendees hear different perspectives on the information needs of different emergency responders, as well as to develop a vision for how information could aid in responding to building emergencies. The draft white paper was used as a starting point with the participants confirming, adding to, or modifying the information contained in the white paper. Issues and concerns associated with the presentation, security and use of building information were also discussed. As a result of the workshop activities, the draft white paper was updated and this is presented in Appendix A. The updated white paper is also available as part of the workshop report which has been published separately (Jones et al., 2005).

The major outcome of the workshop was the identification of information needs for first responders which were broken down into information needs while enroute and on arrival to the incident scene.

Outcomes of the workshop included:

- Identification of the building information needed by emergency responders prior to reaching the scene and on the scene;
- Recognition that the methods used to present this information must be kept simple and should include both audio and visual components;
- Available information enroute must be carefully selected as fire incident commanders typically have very little time to look at it prior to arrival on the scene;
- Use of audio can be extremely useful enroute for those emergency responders unable to view visual information (e.g., drivers, team members in a cab) about the progressing emergency situation;
- Needs for police and emergency medical service (EMS) were discussed and included in the white paper, but additional input was deemed necessary due to the limited number of representatives from these areas.

There was general agreement that the types of information that could be sent to the incident commander would provide more safety and better informed command decisions. There was also

concern that too much information would lead to information overload. There was some discussion about presenting building information in 3D formats. Short text messages were also suggested as useful in addition to graphic display icons. The full workshop report (Jones et al., 2005) is available from the project website.

3 Building Tactical Information System Components

3.1 Building Information Server

Modern buildings contain many sources of information of tactical significance to first responders. These include traditional sources of building alarms and status messages such as fire panels, building automation systems, elevator control systems, and others. Increasingly, they also include repositories of building descriptive information such as construction and occupancy type, floor plans, system schematics, and locations of critical features such as fire department connections, fire panels, building control systems, and others. In some jurisdictions, local fire services may have already prepared some of this building descriptive information for some buildings in the form of pre-emergency plans but most services don't have access even to this limited amount of information.

The purpose of a *building information server* is to provide access to all of this tactical information for first responders before they ever enter a building. An overriding goal is to provide a common "look and feel" to the information irrespective of the specific building, since a given first-responder service may be responsible for hundreds or thousands of buildings (and more than one building may be involved in an adverse event), and irrespective of the specific class of first-responder service, since a given adverse event may require the services of fire, medical, police, hazmat, and other services both local and distant. Desirable features of a building information server include:

- forward alarms and status messages as they occur;
- deliver building descriptive information that establishes context for the alarms and status messages and supports tactical planning and operations;
- allow only authorized access to the server;
- allow authentication of the server by the accessing system;
- allow multiple, independent accessing connections;
- allow asynchronous access to the server; that is, a first responder's system need not be connected to the server before an adverse event begins and may disconnect and reconnect without loss of tactical information;
- provide the tactical information in a common format, independent of the specific originating building systems and their possibly proprietary messaging syntaxes;
- provide the tactical information in a common format that allows for its use in a variety of first responder applications;
- minimize the volume of transmitted information both to maximize the throughput of the server in the face of rapidly changing building conditions and to reduce the load on the communications channels used by first responders;
- make maximum use of the layered communication-protocol approach so that tactical information can be delivered through a variety of communications channels including plug-in connections at the building, dial-up connections, Internet connections, cell-phone messaging systems, and digital radio connections; and
- fail gracefully, that is continue to deliver as much tactical information as possible even as some building systems fail or lose connectivity.

The building-information server approach developed in this project is an event-based message passing system based on the publish-subscribe paradigm. This development is described in detail elsewhere ["Cybernetic Building Systems and Publish-Subscribe Technology: Informing First Responders," Kent A. Reed, NISTIR, in preparation].

Publication and subscription are used in two ways in this approach. Building information systems within the building subscribe to the server for the purpose of publishing alarms and status messages to the server as they occur. This internal subscription process allows the server to authenticate its sources and to know at all times what information can be made available. First-responder applications subscribe to the server to receive messages as they are published by the server. As part of this subscription process, building descriptive information optionally is provided in administrative messages to the first-responder application based on its indicated capability. A journal maintained by the server allows for the transmission of message logs to applications that subscribe after the beginning of an adverse event. The server also ensures that every message contains a valid time stamp and provides an administrative "heartbeat" message so that subscribing applications can know when it is not available. Either by itself or in conjunction with other building network components, the server acts as a firewall between the external applications and the internal systems.

In this approach, subscribing applications could reside in an emergency communications center (911 dispatch), a fire house, an on-site command center, on mobile data computers and personal data assistants, or even in regional or national emergency management centers. Each application could subscribe and unsubscribe as necessary, and each could process the building messages as appropriate.

In order to facilitate this wide usage of building messages, the message format chosen for this project is based on the extensible markup language (XML). While use of this markup approach can lead to larger message sizes, and hence clashes with the desire to minimize the volume of transmitted information, it can substantially increase the reusability of the information contained in the messages. It also makes easier the processes of mapping the messages from internal building information systems, which may be legacy systems generating messages in proprietary formats, into a common open format and of mapping the messages into desired presentation and decision-support tool formats in the first-responder applications. The proposed message format is described elsewhere ["Cybernetic Building Systems and Publish-Subscribe Technology: Informing First Responders," Kent Reed, NISTIR, in preparation]. In its barest form, without regard for a variety of issues surrounding the creation of robust XML vocabularies, an example message fragment published by the server might look like the following:

```
<BISmessage>
<class>alarm</class>
<id>123456789</id>
<datetime>20051215T151020</datetime>
<location>'/third floor/hallway b/room 310'</location>
</BISmessage>
```

The id element allows fully-capable subscribing applications to place this alarm message in the context of the building descriptive information and manipulate the combination to create meaningful graphical presentations and to support decision making. The location element allows even minimally-capable subscribing applications to report to a first responder the fact that the alarm has occurred. Note that the building is not explicitly identified; this information is dealt with at a different level.

Draft message elements have also been developed for some of the building descriptive information identified in the workshop discussed in Section 2, notably for the summary level information that is now typically found on the cover sheets of building design drawing sets,

including construction type and occupancy type, number of stories, methods of fire protection, and the like.

The workshop also identified a need for more detailed building descriptive information comparable to the information found today in a building's architectural floor plans, mechanical system drawings, and project specifications. A decision was made in this project to align work on this building descriptive information with the emerging Building Information Model (BIM) approach based on the Industry Foundation Classes (IFC) data model. The BIM approach provides for a seamless flow of information from the building design team through the cognizant building code official to the building construction team and then into the hands of the building owner or operator. The advantages of this approach include improving and expediting the review and approval of building projects by building code officials and fire marshals, making approved building descriptive information available immediately to fire services and other first responder organizations for familiarization and training even before the building is a reality, reducing the amount of investigation and rework required to create pre-emergency plans, enabling the immediate update of building descriptive information by the owner or operator as the building changes, and leveraging the standardization work already done in the design and construction communities.

Since a fully populated BIM contains far more information than is needed by first responders, a reduced BIM (rBIM) approach has been advocated in this project and parallel studies at NIST. Progress toward creating a prototype rBIM is described elsewhere ["Toward a Reduced Building Information Model (rBIM) for First Responders," Kent A. Reed, NISTIR, in preparation]. In the building information server developed for this project, the building descriptive information was stored in a companion information repository but in a real implementation it likely would be stored in multiple locations for improved system robustness during adverse events.

The Internet TCP/IP suite was chosen as the base communications protocol for testing and demonstrating the server approach developed in this project using the NIST Virtual Cybernetic Building Testbed (VCBT) which is a building simulator that couples actual building controllers for HVAC and other building systems to a computer simulation of a building. The technology for creating gateways between TCP/IP and other communications protocol suites is well established. In this project, one gateway service was exercised to make messages available to cell-phone messaging system subscribers, but others could be used as required to meet the needs of the first-responder community.

3.2 Decision Support Tools

There are many decision support tools already in use with building systems. An example of such a tool would be a smoke detector sensor that has the ability to determine whether it needs cleaning, is in trouble, or is detecting a fire based on analyzing its sensor signal. Decision support tools for emergency responders can be as simple as showing where smoke sensors are in alarm on a floor plan or can require quite complicated calculations to yield information such as how large and where the fire or fires are in the building, the location and depths of the smoke layers in each room, and the impact of activated sprinklers (if present) on the fire.

The Sensor Driven Fire Model (SDFM) described in section 3.2.1 is a decision support system that is being developed in order to experiment with what information can be reliably extracted from fire sensor signals. Other decision support systems that could supply information of value to first responders would use building sensors to evaluate the safety of elevators, the condition

and use of the HVAC system for smoke evacuation, and the location of emergency responders and occupants of the building.

3.2.1 Sensor Driven Fire Model (SDFM)

The SDFM is a prototype decision support system that converts sensor signals from fire sensors to predictions useable by first responders. The SDFM is computer modeling software that has the capabilities to provide the following analysis:

- uses heat, smoke and gas sensor signals to identify and define fire growth and size;
- performs real-time analysis of smoke and fire spread for multiple room structures;
- provides hazardous condition warnings for first responders;
- handles multiple fires that start at different times;
- identifies open/closed door status based on fire system sensor signals to provide real-time building configuration information.

The SDFM is currently configured to operate in the following manner. Signals from either smoke or heat sensors are analyzed based on signal size to determine whether the sensor condition is normal, trouble, or in alarm. If the sensor is in alarm, then an analysis is done in order to determine the potential fire size that caused the alarm. If the calculated fire size is too small and the sensor signal has not reached a predetermined signal size for alarm, no alarm is issued. Otherwise, a fire warning for the space is issued and the SDFM proceeds to calculate increases in fire size and projects the smoke spread on subsequent calculation cycles. The current calculation cycle is every 10 s.

As the fire grows, other sensors will be tested in the same manner with sensors that are responding with signals larger than expected indicating either a spreading fire or new fires. Rooms containing fire sensors that are not providing elevated signals will be assumed to have closed doors if the calculation suggests that an open door would cause an elevated signal for that sensor.

The model provides the following warnings that can be shown as a series of colors on a building floor plan. The first warning is a cool smoke layer that is located 2.0 m above the floor. The purpose of this warning is to alert first responders that this area may present visibility problems. The second warning level occurs when the smoke layer has descended to 1.5 m above the floor and reached a temperature of 50 °C. At this point, the smoke layer is dense enough to be toxic and breathing apparatus will quickly become necessary. The third warning occurs when the smoke layer reaches a temperature of 500°C. At this point, flashover can occur and these spaces need to be evacuated as quickly as possible.

The SDFM currently operates within the Virtual Cybernetic Building Testbed (VCBT). The net result is that building systems can be studied in the framework of a simulated building to understand how these systems would operate.

3.3 Information Presentation

3.3.1 Enroute and On-site information presentation

Based on the initial work spent developing the White Paper and the results from the First Responder Workshop, the need for both enroute and on-scene information presentation screens was established. As envisioned, the enroute screen would provide information about the area surrounding the building and the building shell but would not include information about the interior of the building other than the approximate location on the building footprint where the

incident was located and the presence of unusual hazards. The information presented on this screen must be simple to understand and be supportive of the type of information required by the incident commander for staging and for managing other activities conducted outside the building during the incident. The requirement for simplicity is important as the incident commander typically has only 3 min or 4 min to make staging decisions between the time leaving the firehouse and arriving at the scene of the incident.

The on-scene screen would contain a wealth of information about the interior of the building based on the building floor plans and contents. Information from pertinent building systems, output from decision support systems, and locations of stairs, standpipes, and a variety of other static building information would be available for display on this screen. The organization of this screen is extremely important in order to provide this information in a useable fashion for the incident commander.

Enroute and on-scene information screens were tested in a demonstration (see Section 3.4) with a virtual incident staged in Building 226 located on the NIST campus. The purpose of the demonstration was to provide a first examination of the information system for first responders in a situation where both the NIST police and firefighters could comment on the implementation.

3.3.2 NEMA proposal

A proposal based on the above work (including information content and display organization) was prepared and submitted to the National Electrical Manufacturers Association (NEMA) Signaling, Protection and Communications Product Group/Fire Alarm Group for their comment and adoption into their manufacturing standards and subsequent inclusion into the National Fire Protection Association standard NFPA 72 (National Fire Alarm Code). A copy of this submission is found in appendix B. In December 2005, NEMA published the *Standard for Fire Service Annunciator and Interface* (SB 30-2005) that captured many of the features for the on-site information screen. A second presentation was made to NFPA 1221 (*Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*) at the committee chair's request for consideration of changes required for 911 operations. The presentation is provided in Appendix D.

3.4 System Demonstration

In fulfillment of one of the project deliverables, a demonstration of the intelligent building response technology was performed in February 2005. The demonstration scenario was that of a real response to a virtual incident in Building 226 on the NIST campus and involved NIST fire and police personnel. This demonstration served multiple purposes—demonstrating a technology path for moving data from building to first responder, and providing an opportunity for NIST police and fire personnel to comment on the implementation of the technology and see its potential.

The technology demonstrated included: building sensor data and fire modeling data formatting in XML schema; transfer of building data to a building information server using publish subscribe technology; user software client that subscribed to the building data stream available at the server; and user interface software that parsed and displayed the data to emergency responders. A more detailed discussion of these elements is presented in Appendix C.

A video was produced documenting the NIST demonstration, and this is available in MPEG-1 format online at the iBR website [http://www.bfrl.nist.gov/ibr/] as well as on CD by request.

4 Information security

4.1 Introduction

As part of this project, BFRL was tasked with addressing the information security requirements for building data along the path from building sensor to the first responder (or other public safety official) on the public safety network. The goals of this section are to:

1. Introduce information security goals as they pertain to building response;
2. Discuss some security issues related to connecting the building to the public safety network;
3. Put the security issues for building information into the context of the SAFECOM mission (wireless interoperability for first responders);
4. Outline security requirements for different classes of building data for different users on different networks; and
5. Frame security issues in a holistic manner using the Common Criteria Protection Profile construct.

While this section addresses specifically the security requirements for building information on the public safety network in the context of a building emergency incident, the subject of security and privacy of public safety communications itself has been studied before. Several documents in the late 1990s examined the security issues associated with the newly deployed digital land mobile radio (DLMR) systems. The *DLMR Security Problem Statement* (PSWN, 1998) notes the increased risks associated with computer based radio systems with expanded functionality such as mobile computer access to sensitive databases using the unsecured radio channels. A *LMR System Recommended Security Policy* (PSWN, 1999) document gives a detailed analysis of the radio communication system security risks and recommends policy for addressing these risks. It is written at a fairly general level that is not technology specific, and it addresses administrative security issues as well as computer, communications and radio security. The report recommends the use of encryption on all communication. It serves as a good companion document to this section. A *Security Issues Report* (PSWN, 2002) addresses the complex issues related to the use of encryption. The main conclusions are that cost, maintenance, and encryption key issues are preventing easy adoption of encryption now. Other issues include the public's right to be informed about emergency response activity and performance, as well as interoperability problems when using encryption.

4.2 Information security and building response

Information security is generally presented in terms of device authentication, user authorization, and data integrity and privacy (encryption). The goal of authentication is to ensure that when one device interacts with another device that each side is confident of the identity of the other device. This prevents exchanging data with potentially malicious devices. Authentication is usually accomplished by the use of a shared secret key which is used to sign a message.

The goal of user authorization is to ensure that only those individuals who should have access to certain data *do* have access to that data, while other individuals do not have access. Access may be constrained by time and location as well as user identity. This role-based access control is usually accomplished by a centralized management system that compares username and password (or other form of identity verification) to an access rights database.

Data integrity encompasses the need to guarantee that data transmitted from one device arrives unchanged at the receiving device. This is accomplished generally by attaching a signed message

digest of the message contents to the message. Data privacy is accomplished by encrypting message contents using some shared secret, generally different from the shared secret used for authentication purposes.

In terms of public safety official access to building incident information, the goal is to limit data transfer to that needed by authorized individuals (or systems) at the time needed. Some practical applications of this approach might be:

- Dispatch has access to all incident data as soon as an incident is recognized and for the duration of the incident;
- Fire, police and EMS who have been dispatched to an incident have access to all building information while enroute to an incident and while on scene, for the duration of each individual's involvement;
- All users on the system have to log in with name and password and perhaps biometric and smart card identification;
- All data communication on the network is integrity protected, with end devices authenticated, and sensitive messages encrypted;
- Post-incident investigators have access to needed information while on the case.

4.3 Building network and interface security issues

When considering security of a connection from a building network to the public safety network, security of each separate network will determine security requirements along the whole path from a sensor in the building to a public safety officer on the public safety network. While security requirements of the public safety network have been examined, they have not been examined with respect to the access and use of information from building networks. The main goal of this subsection is to look at existing security on building networks.

The amount of security used in building automation and control systems is determined by building owner's requirements as well as by fire regulations. In many buildings the building control network is completely separate from the IT network, while more recent buildings are likely to have some overlap, with higher level controllers sitting on the IT network using IP communications. Lower level building control devices may use other protocols and sit on dedicated sub-nets.

In general, building network communications are unencrypted and un-authenticated. Some security is effectively provided by limited physical accessibility to the building control network, and authorization of human users prior to permitting them to command certain devices. In addition, the building control network receives some additional protection from the IT network—the corporate network that may overlap with the building network. The IT network is likely to have firewalls in place at its interface to the outside, and may have additional protections within the network. These all provide some security to building communications. In addition, it is notable that building communication protocols are available which offer secure communications using data and user authentication as well as data integrity and hiding, and these will likely see increasing use and are available as needed to meet requirements of building owners as well as potential demands of the public safety network interface.

In summary, building network data are generally not secured at the source, but can be. Lack of authentication at the data source could present problems if defining strict authentication requirements for data on the public safety network. Practically, most building data are not of a

sensitive nature, and spoofing of data is not likely due to the difficulty of gaining access to the building network.

Following is an examination of the security requirements laid out in the SAFECOM Statement of Requirements that relate to building information access security.

4.4 Security in the SAFECOM Statement of Requirements

In the SAFECOM vision of wireless communications interoperability for emergency responders, as set forth in the SAFECOM Statement of Requirements v1.0 (SoR), security is applied to voice and some data communications on several levels of networks. The SoR defines 3 networks: Jurisdiction, Incident, and Personal. The Personal Area Network (PAN) connects sensors and devices on the person of an emergency responder while in uniform. The Incident Area Network (IAN) exists for the duration of an incident and includes equipment (vehicles) and personnel on scene. The Jurisdiction Area Network (JAN) always exists. During an incident, all personnel at the scene participate in the IAN, and the IAN connects with the JAN as needed for support or to report.

The SAFECOM SoR envisions some building information being made available to first responders: floor plans and plot plans as might be available on a fire apparatus now in paper form. However, the concept of a building information system that provides information during an incident to aid in incident response is not discussed in the SoR v1.0. Thus, while security requirements are given for voice and data transfer over the public safety network, no mention is made of security requirements for accessing building information on the building control network. The BFRL role is to provide input on security requirements for the public safety network access to building information.

4.5 Identification of Building Information, Users, and Security Requirements

This section looks at how building information can be classified according to data class, sensitivity and user needs, and discusses security requirements of that information. The following section examines the wider picture of threats, assets, assumptions, and security objectives related to securing the data path from building to user.

4.5.1 Classification of Data

Static data is building information which changes infrequently, such as the floor plan, location of fire sensors and security sensors, etc. Much of this "blueprint" information is documented on architectural plans and resides in some city permit office archive. Most building owners wouldn't care who knows about where the elevators are or the windows or lights. But most owners would be concerned about the security implications of releasing information on locations of security access panel, utility shut-offs, security cameras, valuable materials, hazardous materials, telephone numbers and occupant information. Still other building owners may desire that nothing is public, say for some government facilities (e.g., Camp David or CIA headquarters). For this reason, access to static information via the public safety network must be limited to authorized individuals associated with a building incident, at least if the static information is identified as sensitive by the building owner. Alternatively, the data may be encrypted, or simply not made available outside the building.

Dynamic building data are the real-time sensor data generated during an incident and are sensitive because they are potentially evidence in a criminal investigation. Where did the fire start? Where did the intruder enter? What was seen on video? Did the system believe the sprinklers were on?

Why wasn't smoke vented from a certain zone? Which elevators were used when? While static information exists at all times and may be accessed at any time from a building by an authorized user, dynamic data become available as an incident progresses and then is archived after that. This dynamic data archive must be protected from modification and loss, and only authorized individuals should have access to it.

Data can also be classified by building control sub-system. HVAC, elevator and lighting system details might rank as low-security, while the fire and security and phone system details might be given higher security. Of course, floor plans themselves might be sensitive information. The public safety community must be concerned with distribution of this information since release into the hands of criminals or terrorists might result in damage to buildings and harm to occupants, as well as loss of property.

Finally, data can be classified according to what is required by a given user, i.e., "fire data", or "security data". In fact, there is significant overlap in the data sets required by different first responders. This issue is discussed more below in the next section on user roles.

4.5.2 User roles

This section looks at the potential for classifying data according to user roles in order to protect the spread of data and aid in user authorization. The first subsection looks at the roles of the different services, while the second looks at the role of an incident commander and his/her information needs versus a non-commanding responder.

The premise here is that data can be classified according to a standard classification scheme. This scheme must be implemented in each building's information server configuration in order to identify a set of data for "fire" or "police" or "medical" or "incident commander", etc. It will likely be difficult to draw the line on what data should be restricted for this fine-grained level of data authorization, especially given the complexities in different incident scenarios. And, after performing this exercise of examining how data might be classified, the end conclusion is likely to be that the benefits of having information available to all responders outweighs the increased security from classifying data and limiting access. Examination of threats present in different scenarios will aid in determining the usefulness of data segmentation and degree to which data should be segmented.

4.5.2.1 Fire/Police/EMS

The workshop report (Jones et al., 2005) lists information that is desired by fire, police and EMS, based on input received from each public safety community. There is considerable overlap: police will need to know at least high-level details about a fire situation, and fire responders will want high-level info on any concurrent security incident underway. EMS needs a wide view on the incident site, with specific details related to locating and treating injured people and data concerning ingress and egress from the building. Specific details of what each service needs can be found in the workshop report.

4.5.2.2 Incident Commander vs. First Responder

Is it reasonable to limit some data access to incident commanders (IC)? An IC has command responsibility and must monitor the situation and direct resources while a first responder takes orders and deals with a fire or other incident. The IC needs all the information, potentially, while the firefighter or police officer or emergency medical technician (EMT) does not. Since the non-commanding first responder doesn't need all the information, why give him/her access to it? For

security of the information, is it reasonable to limit the ability of the first responder to access some of the building data?

As indicated earlier, there are pros and cons of limiting data access. If all emergency responders are given access to all the data, this will increase the risk of leaking the information due to: human error, poor training, increased number of user accounts and devices with access that can be stolen or hacked. On the other hand, if access is *not* given, there will be negative consequences as well arising from a first responder not having access to needed data on some occasions. For example, if fire system information is only provided to the IC or to fire personnel, but a police officer is first on scene, then the police officer may be prevented from mitigating the fire while it is small.

One option is that user authorization not be used to control data access at the incident scene, but rather that all public safety communications devices (PSCD) be authorized to view any incident data for which the device has a user interface. That is, it is assumed that only an authorized user will have access to a PSCD. And the device that an emergency responder holds (or otherwise works with) will depend on his/her role. The responder going into the building may only have a radio, or a small PSCD with very limited data access and user interface. An incident commander will have a computer with access to all the data. During an incident each responder must be logged on to the network and authorized to respond to a given incident and thus receive building incident data on his/her PSCD. Any properly authenticated PSCD should have access to any building incident data.

One exception to this may be the opinion of the building owner. Some particularly sensitive building information, according to the building owner's definition, might be tagged for special classification. This sensitive information may require encryption or alternatively may be made available only within the building and not released to outside responders.

Beyond *access* to data, there is also the issue of *control* of the building systems from outside the building. Control of building systems from a wireless node on the IAN is not a near-term goal; with the current publish subscribe server implementation the user can only request some subset of the data. A later generation of the system may give control capability to the IC to open doors, turn on lights, or take other actions. Perhaps a police chief at an incident could disable phones or power from outside the building, etc. So, while access to data may not be determined by user role, control of the building would be limited to the IC/Chief role.

The issues of data classification and user roles will need further discussion as systems are developed and tested.

4.5.3 Summary of Building security

There can be several ways of classifying building information. The building information can be classified cleanly along the lines of pre-incident (static) data and incident real-time (dynamic) data. The first set consists of architectural plans and control system details, some of which would be considered sensitive by the building owners. Required security of static or dynamic data might be roughly classified along control sub-system lines. For example, HVAC, elevator, and lighting might be classified as low security, while fire, security, and phone systems might be classified as high security.

For the real-time sensor data during an incident, all data might be considered sensitive due to the potential for those data to serve as evidence in a criminal investigation. Even the HVAC, elevator,

and lighting systems sensor signal histories must be regarded as sensitive information—in the SAFECOM SoR, text and image data communication of similar sensitivity is given the special constraints, "much of this data needs to be encrypted to protect privacy concerns and ongoing criminal investigations" [SoR v1.0 section 4.4.7.1, Table 26]. Privacy is mainly a concern when building occupant information is exchanged.

Therefore, if the concern of the SoR to protect data for evidentiary purposes is transferred to building information, then *all* real-time sensor data must be protected, with access limited to authorized individuals, and data encryption used on much of the data both during the incident and in storage after the incident. Considering the sensitivity of some static data (details of security system, location of cameras, etc.), it is likely that some of this data must be encrypted as well. On the other hand, authentication may be all that is required, or allowed due to practical system considerations.

All the issues relating to encryption on the public safety network, as outlined in *Security Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems*, PSWN Program, March 2002, apply here as well. Assuming that encryption is standardized, key distribution across domains addressed, and guidelines given for release of data via Freedom Of Information Act requests, then encryption of data streams can be made possible.

The following guidelines are recommended for securing building information and the connection of the building network to the public safety network:

1. Rely on data authentication (digital signatures) to ensure that data have not been modified for investigation purposes.
2. Encrypt information that is identified by building owner as sensitive. If encryption is not available, then building owners can limit data made available to the public safety network.
3. Provide role-based access control to PSCD devices to ensure that the right users have access to needed data, and avoid pitfalls of individuals viewing or acting upon data when they are not authorized or trained to do so.
4. Archive all building data (static and dynamic) that are made available by the building from start of the incident until conclusion, for the purposes of post-incident investigation and training.
5. Include building information and consider security of the building data and networks in the development process of any public safety network, and provide a secure path for moving building information from building information server to each public safety official who could benefit from that information, providing it at the proper time in an understandable format.
6. A "public safety network to building interface security requirements" document needs to be developed as the security requirements of the public safety network become clearer. This document would inform public safety officials and building owners about the above requirements and ensure that both the public safety networks and data as well as building networks and data are protected during and outside of building incidents.

Additional requirements are outlined in the Security Objectives in Section 4.6.5

4.6 Threat assessment and security objectives

The SAFECOM Statement of Requirements is written from the public safety officer's point of view—listing functional requirements. It does not try to address the system architecture that can meet the requirements. It also does not try to justify the requirements. Such a justification could

follow the format of a Common Criteria (CC) Protection Profile (PP) that defines a Target of Evaluation (TOE), then lists assumptions, assets, vulnerabilities, attackers, threats, security objectives, IT security requirements to meet those objectives, as well as policy requirements. An analysis in this CC PP format of the assumptions, assets, vulnerabilities, attackers, threats, security objectives, and IT security requirements of the path from building sensor to first responder display is presented in this section.

4.6.1 The System Target of Evaluation (STOE)

1. The STOE is the path from building sensor to first responder display. Examining the path will determine whether the security on the building control system and public safety network meets the conditions required for transfer of building information.
2. The STOE includes the building information server, which is the interface between the building and public safety network; it is an add-on to the building control system that gathers needed building data and serves it up to the public safety network.
3. The STOE does not include security of the IAN (Incident Area Network, as defined in the SAFECOM SoR) or JAN (Jurisdiction Area Network) in general, but only the use of building information on those networks, i.e., security of the information transfer from building server to authenticated user on the IAN or JAN, and security of the end user's graphical interface or other application. A security policy for land mobile radio systems was prepared for SAFECOM in 1999 [PSWN, 1999] which addresses strictly radio (primarily voice) communications security.
4. Detailed Scope (adapted from System Protection Profile – Industrial Control Systems, Decisive Analytics, 2004):
    a. Physical protection of hardware and network cables in building
    b. Network security of sensor (dynamic) and other building data (static) along data path and in attached components
    c. Building data authentication and encryption (as needed)
    d. Authentication of public safety personnel requesting access to building data
    e. Continuity of operations (backup and power for building network and IAN)
    f. Operating procedures (procedures for security and continuity)
    g. Personnel management policies
    h. Training

4.6.2 Assumptions

The following assumptions are made regarding the STOE security environment:

1. Data are only available during an incident. While authorized individuals can request static data at any time, real-time sensor data are only available when an incident is under way, and afterwards the data record is safely secured and not accessible except to authorized users. Eavesdropping on unencrypted data will only be possible during an incident.
2. The building control network has physical security measures, as well as network security measures in place to limit access from outside and extent of any one user's access to services and devices when logged on the network.
3. The public safety network has network security measures in place (as specified by SAFECOM), but only has minimal physical security on equipment due to the temporary and accessible nature of the network.
4. Men and women in uniform are not fully trusted. Any human can make mistakes. There is also some risk of a rogue first responder abusing privileges, endangering others, misusing information.

4.6.3 Assets

1. Building sensors, with more value placed on and protection required for fire and security sub-systems than other sensors.
2. The building sub-system controllers responsible for collecting and transmitting data to the building server.
3. The building information server that gathers building data and accepts subscribers to that data.
4. Building communications infrastructure: other network components within the building control network.
5. The software components along the path from sensor to end-user, including programs running in the building information server as well as first responder user interface(s).
6. Public safety communications infrastructure: network components within the public safety network (IAN, PAN).
7. The static and dynamic building data itself.

4.6.4 Threats

The SAFECOM SoR cites protection of evidence as the reason for requiring privacy for voice and some data communications. The additional issue of a building owner's interest in protecting sensitive information was raised above. What are the real threats that touch on these points? The following list addresses threats as well as vulnerabilities, threat agents, and possible attack vectors.

1. Eavesdropper
    i. Possible eavesdroppers
        i. Reporters: in any important incident there will be reporters close to the scene, and they are interested in following the events first-hand, rather than via a public relations agent. They may publish/leak sensitive information.
        ii. General public—They may leak evidence as well, or cause other trouble.
        iii. Insider—disgruntled employee or former employee, whether first responder or other authorized public safety official, might use information for any and all kinds of evil purposes (disclose, modify, and destroy information; destruction of property; tampering with equipment; theft; etc.)
        iv. Criminal or terrorist: Suppose a criminal pulls a fire alarm simply so he can receive from the building (via the IAN) details of the bank security system and floor plan for use in a later robbery.
    j. Required equipment
        i. Anyone who wants to eavesdrop needs a public safety communication device (PSCD) that interoperates with equipment on scene at an incident. (this could be a radio with a wireless connection at the scene; building data could also be intercepted off a wired network such as the Internet if not secured). The PSCD provides whatever software clients (e.g., the tool to view the 3-D representation of the building) are used to view and make sense of the building data.
    k. Available access: It is likely that the IAN would have signal range extending beyond the security perimeter at an incident. In this case, an eavesdropper could simply sit unnoticed outside the perimeter and listen in on communications.

2. Individual trying to impersonate a first responder
    a. The "hero-wannabe"—would such an individual have access to a public safety communication device? It seems more likely that such an individual might pretend to be a first responder, but without network access. If such individuals do somehow gain access to the network, would they leak evidence? That is not their goal.
    b. Likewise, if terrorists or criminals try to get inside the security perimeter by impersonating an officer, their primary purpose would not be to get on the network (since they could do that from outside the perimeter).
    c. On the other hand, impersonating an officer in order to get access to equipment might be the only way to gain access to the network.

3. Failure of physical security of public safety communication devices (PSCDs). While a reporter probably would not break the law to steal a PSCD, a criminal could. If a PSCD could be stolen, then the thief may be able to receive and view all incident communications. Some safeguards should be in place to protect the devices while in the station, in the vehicle, and at the incident.

4. Compromise of the Building Information Server (BIS). The BIS is in effect a gateway to the building network. It must have all the protection of any other web server sitting on the Internet. It should be dedicated to serving building data to the public safety networks to limit attacks launched by attacking other applications running on the same device. This device is still vulnerable to compromise due to software and hardware bugs, denial of service, misconfiguration, etc. The architecture should be designed such that the compromise of the building network does not allow access to the public safety network and vice versa.

5. System reliability
    a. It is a threat to safety (public safety as well as first responder safety) to have misconfigured networks, PSCDs, etc. Therefore, well developed policies must be in place to govern management. Training must accompany those policies to have standard implementation.
    b. It is a threat to the whole program (and thus the potential gain from the program) if equipment does not perform as expected and responders choose not to use it.

6. Mishandling of evidence, unreliable data.
    a. If data are not properly secured along the path from sensor to display or database, the case might be made that evidence was tampered with or is otherwise unreliable. This would complicate a criminal case or any non-criminal investigation.

7. Management failure. The following elements open the door for network attack:
    a. Failure to set up policies for quality control, network configuration, security measures, application development, training, etc.
    b. Failure to train properly
    c. Failure to do risk assessment

8. Power outage. Power can be lost due to incident itself, malicious intrusion, or human error in shutting off power to control system. With power off, the source of information is lost and first responders lose access to that information.

4.6.5 Security Objectives

1. The STOE must be physically protected to disallow unauthorized access to network components.
2. A risk assessment will be performed initially and on an ongoing basis, examining risk in the context of different IAN configurations connecting to different building control networks at different locations/buildings.
3. The building information server interface shall be implemented such that it does not interfere with the building control network, or with the public safety network.
4. The building information server shall be implemented such that no device on the building network can gain access, or be used to gain access, to the public safety network and vice versa.
5. The building must have policies in place to govern power and continuity of the server interface. Power to the building control system should be on a protected circuit. The server should have back-ups to allow system recovery in case of compromise or damage.
6. The building control network should at minimum require network security that will prevent an outsider from gaining access to the network. In addition, all human users must be authenticated. A risk assessment will guide determination of sensitive devices and services requiring authorized access, e.g., reconfiguration of security system or routers. The risk assessment will also guide use of physical security measures.
7. The building control network shall be protected so as to ensure the integrity of data reaching the public safety network.
8. Integrity (and potentially privacy) of building data must be protected while in transit to PSCD.
9. The public safety network should have policies in place to govern physical access to network equipment, as well as policies to manage power and system continuity in the face of equipment failure or compromise or damage.
10. An overarching security policy will be developed that specifies a security management infrastructure, roles and responsibilities, and training for all users.
11. Policies shall be in place to govern access to building information and building control systems from internal to the building, from offsite, and from public safety network via building information server. This includes roles, responsibilities, and access authorized.

5 Standards Development

This section documents the standards work undertaken by BFRL in conjunction with this project. The interactions with the public safety community and with numerous standards bodies has lead to advancement of standards in several areas including: presentation standards for building information on user interfaces, security of building networks (biometrics and security within the BACnet protocol), and a proposal for a new Public Safety and Emergency Response Domain with the International Alliance for Interoperability.

5.1 Interactions with the public safety community

The initial thrust to interact with the public safety community came with the First Responder Information Gathering workshop (section 2 or this report). Following that were many other interactions.

BFRL staff made several visits to the Montgomery County (MC) Maryland Emergency Control Center (ECC). The first visit focused on understanding the operation of a large county emergency call center operation including: data and applications handled, organization, security, roles, etc. The center has no access to real-time building information other than a fire alarm indication delivered via an alarm company, and some building floor plans stored as PDF files and accessible from their Graphical Information System (GIS) interface. Contact was made with Lt. Dallas Lipp of MC Fire and Rescue, who was leader of the PS2000 program which is the current generation of radio and data network used by all emergency personnel and tied in with neighboring counties. On a later visit to the ECC, Lt. Lipp was interviewed for the video where he shares about the potential use of building information. Lt. Lipp and other senior county emergency services representatives have expressed interest and willingness to participate in new technology demonstrations.

The production of the video itself allowed BFRL staff to make connections and understand the unique perspectives of MC Fire and Rescue (interview with the fire chief, Tom Carr), and Gaithersburg police (interview with police chief Marianne Vivarette, who is now also serving as president of the International Association of Chiefs of Police). In addition to these local contacts, the workshops have given us contacts and perspectives of emergency responders from outside Montgomery County, including large city and rural fire services.

BFRL staff also had significant interaction with NIST fire and police, including learning about the technology used on campus, hearing the perspectives of the fire and police chiefs and discussing building information needs, and working with them in the NIST on-site technology demonstration and video.

Finally, continued contact and cooperation has been made with fire Chief Don Oliver and the Wilson Fire Department of Wilson, NC. Wilson has a reputation as a testbed for the latest fire service technology and has worked with BFRL in the past and continues to participate in technology demonstration efforts.

5.2 Interactions with standards organizations

Throughout the term of this project, BFRL staff had many interactions with standards organizations focused on addressing project goals.

The goals and progressive results of this project were presented to the National Fire Protection Association (NFPA) in May of 2004 and 2005, and to the NFPA Research Foundation in January

of 2004 and 2005. A presentation of this project was presented to the NFPA 1221 (Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems) committee.

Presentations were given in spring 2004, spring 2005, and fall 2005 to the National Electrical Manufacturers Association (NEMA) related to moving building information requirements for first responders toward standards for user interfaces.

Project team members are active on the American Society of Heating Refrigeration and Air-conditioning Engineers (ASHRAE) BACnet committee and have participated in regular meetings addressing security in the BACnet building control networking protocol. A security specification for BACnet was under preparation during the project and has been released for public review. In addition, BACnet is being extended to support access control, and the role of biometrics in building security is being analyzed. Project team members are also participating in related work of the Security Industry Association.

BFRL staff have also been active in standards organizations that preside over building information systems. The National Institute of Building Sciences (NIBS, **www.nibs.org**) is the home for the North American Council of the International Alliance for Interoperability (IAI/NA). NIST is a member of NIBS and the IAI/NA. In order to ensure the alignment of the IFC and BIM activities with the needs of the first responder community, NIST has proposed to NIBS that the IAI/NA create the Public Safety and Emergency Response Domain. This proposal has been accepted.

The Jabber Software Foundation (**www.jabber.org**) has developed messaging technology that has subsequently been standardized by the Internet Engineering Task Force (IETF, **www.ietf.org**) as the Extensible Messaging and Presence Protocol (XMPP). This standard along with the Jabber Extension Proposal for defining a Publish-Subscribe network using Jabber entities is compatible with the work done in this project and the building information server that was implemented for the system demonstration is being re-implemented using XMPP.

The Common Alerting Protocol (CAP) is a standard being developed by the Emergency Management Technical Committee of OASIS (Organization for Advancing Structured Information Standards, **www.oasis-open.org**). The CAP standard defines data interchange for alerting and event notification applications on a regional and national scale. While the project described in this report has focused on local interactions, the approach is consistent with the CAP effort, and alerts generated in the building information server could be forwarded to a CAP network with little effort. The Emergency Management Technical Committee has already defined a profile for publishing CAP messages using the Jabber publish-subscribe network noted above. When the building information server has been re-implemented using XMPP, this profile will be used to demonstrate the interoperability with CAP.

6 Conclusions

It is clear that whatever technology path is developed to move data from a building must interact with the public safety network system architecture under development by SAFECOM. For this reason, BFRL has begun to work with SAFECOM to address the connection of buildings to the public safety network. Part of this effort is in informing the first responder community of the potential for much more intelligent building response to building emergencies, and part of this effort is in incorporating building information transfer technology into the SAFECOM Statement of Requirements and System Architecture Framework. This work has only just begun and will continue into any follow-on phase of this work.

It is also clear that success in collecting and moving building data from the building control systems to the public safety user will require significant additional standards efforts related to classification, formatting, transport, and storage of data in addition to development of a standard interface to the public safety network. This work will require interaction with many standards communities, including:

- Public Safety: fire (working with International Association of Fire Chiefs), law enforcement (working with International Association of Chiefs of Police), medical, computer aided dispatch vendors, communications technology vendors, as well as SAFECOM and other federal, state and local governmental organizations.
- Building information: International Alliance for Interoperability (IAI), Emergency Management Technical Committee of the Organization for Advancing Structured Information Standards (OASIS)
- Building systems: vendors, American Society of Heating Refrigeration and Air-Conditioning Engineers (ASHRAE) BACnet standard committee, National Fire Protection Association (NFPA) and fire regulatory bodies, National Electrical Manufacturers Association (NEMA), Security Industry Association (SIA)
- Building owners: Building Owners and Managers Association
- Mapping: GIS standards bodies and vendors

One proposal for coordinating this complex standards effort across multiple communities is to hold a workshop focused on developing a roadmap for reaching consensus on a variety of needed standards for making the vision of standard access of building information possible.

The accomplishments from this project are:

1. The workshop White Paper that documents for the first time the needs of emergency responders for building information during building incidents;
2. Requirements have been developed for fire panel and incident command display standards and submitted to NEMA These have now been released as standard NEMA SB 30-2005, *Fire Service Annunciator and Interface*;
3. IAI/NA has agreed to create a new Public Safety and Emergency Response Domain.
4. Security requirements for building information on the public safety network in the context of a building emergency incident have been documented (in this report).
5. A method of formatting and transporting building data, using publish-subscribe technology, from building systems to emergency responder displays has been documented and demonstrated (in this report).
6. Several issues have been identified that require further research, including: identifying the minimum set of static building information to present on an emergency responder display (the reduced building information model or rBIM); development of consensus

standards for building information collection, formatting, storing, and communicating across the public safety network; translation of GPS to building local coordinates;
7. Presentations made to various first responder groups, equipment vendors, and standards bodies have raised awareness of building information availability and its potential for aiding in incident response;
8. Two videos were produced to aid in educating these same groups.

7 References

Jones, Walter W., Holmberg, David G., Davis, William D., Evans, David D., Bushby, Steven T., Reed, Kent A., "Workshop to Define Information Needed by Emergency Responders during Building Emergencies", NIST Internal Report 7193, January 2005.

Reed, Kent A., "Cybernetic Building Systems and Publish-Subscribe Technology: Informing First Responders," NIST Internal Report, in preparation.

Reed, Kent A., "Toward a Reduced Building Information Model (rBIM) for First Responders," NIST Internal Report, in preparation.

"Digital Land Mobile Radio (DLMR) Security Problem Statement", Public Safety Wireless Network PSWN Program, available at http://www.safecomprogram.gov/SAFECOM/library/security/ , June, 1998.

"Land Mobile Radio Recommended Security Policy", Public Safety Wireless Network PSWN Program, available at http://www.safecomprogram.gov/SAFECOM/library/security/, October, 1999.

"Security Issues Report—Impediments and Issues on Using Encryption on Public Safety Radio Systems", Public Safety Wireless Network PSWN Program, available at http://www.safecomprogram.gov/SAFECOM/library/security/, March, 2002.

"System Protection Profile – Industrial Control Systems", v1.0, April 2004, prepared for NIST by Decisive Analytics, available at: http://www.isd.mel.nist.gov/projects/processcontrol.

Appendix A Workshop White Paper

White Paper on Building Tactical Information for Public Safety Officials

Introduction

Response to a building incident typically commences with a 911 call. Dispatch provides first responders with the type and location of the incident and determines order of dispatch. A map of the running route will be carried in the emergency vehicles along with building keys and a Knox Box key (a Knox Box is a fire service lock box that is attached to a building and contains the building keys) although not every building will have a Knox Box or keys. When keys are available, they open outside doors, utility rooms and mechanical rooms.

For the fire service, hydrant locations may be indicated on the route map, while the extent of the building information on the map depends on the type and use of the building. For commercial buildings or apartment houses, the map may include an outline of the building and the location of the standpipe/sprinkler connection and door/garage entrances. For newer buildings, the location of the annunciator panel and fire control room is sometimes available. Additional information about the structure may be available in binders carried in the responding apparatus. These preplans may contain interior floor plans, locations of stairwell risers, the location of utility shutoffs, known hazards, etc. Its detail will depend on the person that did the work.

With the development of small, rugged portable computers and compact electronic storage media, the information available to a first responder about a building or other incident can be expanded and made more accessible. Advances in telecommunications have opened up the possibility of supplying first responders with real-time information about the building and incident prior to arrival. Fire departments are moving toward using electronic pre-emergency plans (e-plans) for buildings that can be accessed from computer terminals in the apparatus.

Recent work at NIST has demonstrated the possibility of using building sensors and a decision support system to send information about a developing building fire to first responders prior to their arrival at the building. When added to the information that pre-plans can contain (see NFPA 1620), the amount of building information that can be made available to emergency responders is overwhelming. This paper is designed to start a dialogue that should result in the development of a set of minimum standards for building information provided to first responders while enroute and on the scene of building incidents. The goal of these standards is to provide responders with static (pre-plan) and dynamic (real-time) building information in a format that is readily understandable and is universally accepted such that the use of the information becomes seamless.

An incident can be broken down in time to three general periods. The first period is the time from dispatch until arrival at the incident; typically about five minutes. The second period is the time from arrival until the extent of the incident and method of attack has been determined, and the last period is the mitigation of the incident. The amount of information needed during each of

these periods will depend on the type of incident. The key is to look for commonalities in information across incident types and develop information groups that can be readily displayed on a computer screen.

The next sections explore possible minimum information sets for several different incidents. The information contained in these sections prior to the workshop was based on material from NFPA 1620; pre-fire plan information from several sources compiled and supplied by Santa Rosa, CA, Fire Chief Ronny Coleman; Essentials of Fire Fighting, 4th edition; International Fire Service Training Association; several fire department websites; and discussions with Montgomery County Fire Captain Bob Vettori, Prince Georges County EMS responder John Demarest, fire protection engineer Erica Kuligowski and Fire Chief Don Oliver of Wilson North Carolina Fire Department. Information was also used from the workshop on first responders held in July 2003 at NIST. The following information has now been updated to include input received during the May 2004 workshop, as well as some follow-on information received from attendees of the NFPA May 2004, meeting in Salt Lake City.

A building fire, the first five minutes

The "first due" responder typically has five minutes between time of dispatch and arrival at the incident. The officer in charge must make sure that his team is seated and belted in the apparatus, dressed in turn-out gear, and that all the doors are closed. The officer must then check with the driver to make sure that the route to the incident is known and then uses the route map to verify that the route is correct.

At this point, the officer can start to process additional information about the incident. Due to the difficulty of reading computer screens or hard copy when the apparatus is in motion, the information display must be simple which limits the quantity of information that can be displayed. The information that may be displayed comes in two categories, static or time independent information and dynamic or real-time information.

A building fire – en route – the first five minutes

- Building occupancy (abandoned, vacant, number of young children, high occupancy, number of elderly, numbers of occupants should be based on time of day).
- Building condition (let burn, unsafe to enter, dangerous roof, sprinklered and other suppression systems)
- Building type (single family, commercial, gas storage, school).
- Building style (one story, two story, n story, auditorium, sublevels, etc) include square feet.
- Building construction (type I, II, III, IV or V; fire resistive, noncombustible or limited combustible, ordinary, heavy timber, or wood frame).
- Roof construction (light weight metal or wood trusses).
- Hazardous materials (Unusual hazards) (above ground propane tank, gas lines, chemicals, etc)
- Location of fire hydrants on map with building outline. Nonstandard thread sizes should be noted with the hydrant.
- Location of fire department hookups for sprinkler system/standpipes.
- Other sources of water nearby.
- Location of staging areas and entrances and exits to building.
- History of location in case fire stages before police arrive.

- Routing information for emergency equipment to reach the building in case of construction.

The **dynamic and calculated** information available to the first responder

- Confidence in the incident being real (based on number of sensors in alarm and/or calculated fire size)
- Approximate location of fire within building.
- Fire size and duration.
- Estimated water flow in gallons/minute or foam based on fire size
- Assessment of the local hydrants capability of supplying this water.
- Sprinklers are flowing/no sprinklers or other working systems.
- Fire growth (fast, medium, or slow).
- CBR (chemical, biological, radiation) sensors present and in alarm.
- Police on the scene.
- Presence of occupants in building
- Stairwell smoke/heat conditions for positioning.
- Standpipes to use to get to the fire.
- Exposures.

Other units responding to the scene should receive the same type of information even though it may take them an additional five to ten minutes to reach the incident. The fraction of this information that can be supplied will depend on the building type and age with new, large commercial buildings having the infrastructure to supply most of the points on the list.

On the Scene

Once the first apparatus has arrived, the incident commander will require additional information. For house fires and other small buildings, a visual inspection from the outside and information supplied by occupants would be a first priority. For large buildings, the fire may not be visible from the outside and a visual check may not be a first step. Typically, large buildings have twenty-four hour security or desk people that may provide information on where the incident is located within the building.

Electronic data that would be useful at this time would include a building floor plan and a plot plan of the area. The **floor plan** (static data) would include layers/overlays that would allow the incident commander to locate:

- Key box.
- Doors, windows (with types and which can be used for egress), stairwell risers, fire walls (with ratings and area separation), roof access, fire sensors.
- Security sensors, closed circuit TV cameras, occupancy sensors, security control room.
- Fire alarm panel and remote annunciator panels.
- Utility shutoff.
- Building generator (with indication of what it powers)
- Building system controls (HVAC, smoke control, others), areas covered, special operating systems, and which ones should and should not be used by the responders.
- Persons with special needs.
- Areas of refuge.

- Evacuation quality elevators, floors served, and location of elevator overrides and how to control.
- Convenience stairs/evacuation stairs.
- Areas (zone boundaries) protected by sprinklers or other devices.
- Hazardous materials (type indicated)
- Potential building hazards that may require decontamination.
- Vertical openings.
- Extremely valuable materials.
- Contact number for building engineer.

Dynamic and calculated data that would be useful and could be a series of overlays on the **floor plan** include the following:

- Location of fire detectors in alarm.
- Location of CBR sensors in alarm.
- Location and size of fire/fires.
- Duration of the fire/fires.
- Location and condition of smoke.
- Presence of smoke in elevator shafts or stairwells.
- Identification of activation of sprinklers or other devices.
- Location of elevators used during incident.
- Location of people in need of rescue (911 calls or visual sightings).
- Warnings of structural collapse based on material type, fire location, fire size and duration.
- Location of operational elevators.
- Alarm, occupant, and system histories of building.

The **plot plan (outside building)** would be resizable and contain the following information:

- Building location with street designations.
- Location of fire fighting obstacles such as street widths, overhead clearance and elevations.
- Location of underground pipelines and other utilities.
- Name and phone numbers of building owners and managers.
- Name and phone numbers of utility contact people.
- Location of police line necessary to isolate the incident.
- Indicated runoff or water table problems.
- Helicopter landing areas.
- Evacuation routes.
- Bomb blast radii for buildings.
- Chemical/radiation staging.

Dynamic data that could be displayed on an overlay of the **plot plan** would include:

- Location of responding units (fire, police, and EMS).
- Location of units responding but not yet on scene.
- Hospital availability.
- Helicopter availability.

- Hazmat response.
- Location of police line necessary to isolate the incident.
- Location of triage or evacuation area.
- Suggested hazard perimeter.
- Local weather conditions and predicted spread directions.
- Wind direction and velocity.

Additional data that may be needed concerning the incident include a long list of contact numbers for public safety or relief agencies.

Medical Emergency

A medical emergency within a building can require a subset of the information needed for a building fire. For large structures, the location of the victim and how to get to him/her is of primary importance and a simple floor plan becomes very useful. On dispatch, a route map and a simple plot map showing the outlines of buildings and adjacent streets would be useful. Upon arrival at the building, a simple floor plan containing the following static and dynamic information would be required.

The e-plan floor plan display should include the following static information:

- Doors and stairwell risers.
- Elevators with elevator cars designated for ambulance stretchers.
- Building hazards that may require patient decontamination.

Dynamic data that would be useful include:

- Nature of medical emergency and estimate of need for patient transportation.
- Location of patient.
- Quickest route in building to location.
- Victim data including age, size, sex, allergies and pre-existing medical problems.
- Police on scene.
- Hospital availability.
- Helicopter availability.

Police Action

Building information that would be useful for an incident involving a break-in or other criminal incident would require a building floor plan with different sets of sensor data than would be used for a fire. Static data that should be included consist of a building floor plan and plot plan and a route map.

The building floor plan should include the location of:

- Key Box.
- Doors, windows and stairwell risers.
- Security alarm panel and remote annunciator panels.

- Utility shutoff.
- Hazardous materials (and types).
- Motion detectors.
- Surveillance cameras.
- Security office.
- Security zones and door access point locations with type of security (key, card reader, biometric device, RFID reader)
- Telephones and corresponding phone numbers.

The plot plan should include:

- Building location with street designations.
- Building occupancy (abandoned, vacant, young children, high occupancy, elderly).
- Building type (single family, commercial, gas storage, school, etc)
- Building style (one story, n story, n story with basement, auditorium, etc).
- Name and phone numbers of building owners and managers.
- Name and phone numbers of utility contact people.

Dynamic information from sensors that would be involved with security would include:

- Door access history, location and progress on intrusion.
- What security devices were operated (tripped) and their location and time of operation.
- Lighting and elevator use history.
- Location of activated motion sensors and other security sensors.
- Surveillance cameras.
- Confidence in the incident being real.

As police respond to a building alarm, bringing up this information electronically either within the responding patrol car or at the police station would provide the responders with a tactical advantage compared with what is now available.

Summary

This list of information represents a first cut for electronic information available at an incident. In particular, needs for police and EMS were discussed and are included here but additional input is needed due to the limited number of representatives from these areas. While additions and subtractions to this list are expected over the next months, a next step is to decide how to order the information by electronic screens and standardize the symbols used on the displays. An excellent starting point is NFPA 170, Standard for Fire Safety Symbols, and NFPA 72 annex, National Fire Alarm Code. A subset of these symbols should represent a starting point for the e-plan standard. There are several companies developing GIS based software that is being used for preplanning by fire and other public officials and the good ideas in their products should be incorporated in the standard.

Discussion of the display of information led to the following conclusions. The methods used to present this information must be kept simple and can include both audio and visual presentations. Audio can be very beneficial in communicating to a first responder who must watch the road, or to others in a vehicle who cannot see a visual display. Specific phrases used in audio messages

should be standardized. The use of colors on displays needs to be explored as an aid in recognition of information. There was some discussion about presenting building information in 2D or 3D formats, with participants agreeing that need for 3D information was limited. The use of icons in some instances was also suggested but short text messages could also be effective. A set of symbols is useful for the video display and would include:

- Drop of blood for a medical hazard
- Skull and crossbones for hazardous materials
- Life safety for a person
- Fire symbol for a fire
- Gun symbol for shots fired
- Bomb symbol for a bomb.

Finally, available information enroute must be carefully selected as the incident commanders typically have very little time to look at it prior to arrival on the scene. There was general agreement that the types of information that should be sent to an incident commander would provide more safety and better informed command decisions. There was also concern that too much information would lead to information overload.

Appendix B NEMA proposal

The following report was prepared and submitted in April 2005 as a proposal to the National Electrical Manufacturers Association (NEMA) Signaling, Protection and Communications Product Group/Fire Alarm Group for their comment and adoption into their manufacturing standards and subsequent inclusion into the National Fire Protection Association standard NFPA 72 (National Fire Alarm Code).

Recommended Information Set and Interface Design for use by First Responders during Building Incidents

Introduction

The focus of the current Building Tactical Information System project at NIST Building and Fire Research Lab is to identify building and building related information that would be useful to first responders (fire, police, EMS) and then to determine a method for providing that information to first responders. This proposal presents two pieces of that data path, namely the information required by first responders and the displays that present the information to first responders.

The proposal is divided into two sections. The first section focuses on the information content. The second section presents an example of how the information might be effectively presented to the first responder on a user interface. Note that, unlike current information displays that are attached to the building (i.e., the fire panel), the information displays envisioned here make this data available through the public safety radio network and the Internet.

Section I Recommended Information Set for Building Incident Response

The purpose of this section is to inform manufacturers of the essential types of information that can help insure the timely rescue of occupants, reduce the loss of life and property, and increase the safety of first responders. The source of this information is the output of a workshop held at NIST in May 2004[1] together with results of work following that workshop. The goal of that workshop was to communicate with first responders the information that is potentially available from a building, and to get their input on what information they feel is most needed at what times.

The workshop itself was heavily weighted toward the fire community, with less representation from police. There was also minimal input from the emergency medical community. The

[1] Walter W. Jones et al., "Workshop to Define Information Needed by Emergency Responders during Building Emergencies," NIST Internal Report 7193, Jan. 2005, for workshop held in Washington DC in May 2004.

information presented here exceeds what should be available at a fire panel. Not only are we addressing information potentially available from multiple building control sub-systems (fire, security, lighting, elevators, HVAC), but we have included information related to the building incident that may not come from active building systems, such as floor plans, plot plans, hazards, building incident history, and information gathered from 911 calls.

The information presented is all information desired by first responders. It has been organized by availability, with information that can be obtained with current technology classified as "Required" (Tables 1, 2, 3), while information that depends on future technological advances is listed as "Future" (Table 4).

Within Tables 1 through 4, information is presented in a columnar format:

1. Column 1 (leftmost) is the information element.
2. Column 2, "When needed", indicates whether the information is required enroute or on-scene or both.
3. The third column, "Data source", indicates the *likely* information source:
    - **City** (municipality) indicates data not specific to the building that would likely be maintained/ provided by the municipality or the fire department (FD) within the municipality and might include: GIS system information, traffic information, hazards information, weather, etc.
    - **BIM**—the Building Information Model, which is a database of relatively static building configuration information. This includes floor plan information, location of standpipes, hydrants, etc. This information originates from the architect and is approved by the Building Code Official, but also includes changes in the building over time such as permitted changes (e.g., renovation), changes noted by the owner/operator (e.g., during maintenance and upgrades), as well as changes noted by fire department in regular inspections (fire department changes are indicated in the tables with BIM/FD).
    - **BAS**—the Building Automation System, which is the nerve center of the building and includes fire panel and other building control and monitoring sub-systems. Here, BAS signifies real-time sensor data (such as alarm events, elevator status, etc.), whereas BIM signifies static data that is not incident specific. However, any element that suggests both a location and a status likely will be sourced from both the BAS and the BIM.
    - **DSS** (Decision Support System)—indicates an information element for which all or some part is a calculated value (such as fire size or occupant location) produced by a software application analyzing real-time sensor data (including historical data if needed).
    - **IC (Incident commander)**—indicates data entered into the system on scene by the Incident Commander.
    - **Dispatch**—indicates input about the ongoing incident provided by a human operator, rather than automated data retrieval.
4. The fourth column, "Service", indicates which emergency service is more likely to use the information (fire, police, EMS), and the last column gives any applicable notes.

It is important to note that there are two fundamentally different time periods to response (enroute and on-scene) and that these two periods require different interface displays (discussed in Section II). These two time periods correspond approximately to two views of an incident, the wide-perspective map view (Plot-plan, the primary interface enroute) and the focused building view (building display, the primary on-scene display). Table 1 includes all the required enroute information. Table 2 focuses on the required on-scene building display information. Table 3 lists

on-scene information for the plot-plan display, which should be presented on-scene in addition to the "on-scene" information elements in Table 1. Table 4 is information that is needed[2] but may require additional technology development or is information that is not routinely gathered.

After Table 4, the information of Tables 1-3 is presented again organized by data source (column 3 of Tables 1-3) in order to see this break-out more clearly.

[2] ibid.

Table 1 Required enroute information elements (to be shown in plot-plan display)

Information element	When needed	Data Source	Service	Notes
Map of area showing location of the building, street names	Enroute/ On-scene	City	All	Current GIS systems
Name and address of building	Enroute	City	All	At initial alarm, building ID must come from building
Identification of type of alarm: fire, security, CBR (chemical; biological, radiation), other. List all classes of alarms present.	Enroute	BAS/ Dispatch	All	Based on type of sensor in alarm or called in information
Confidence of incident being real (based on number of sensors in alarm)	Enroute	BAS/DSS	All	
Alarm duration (time elapsed since first alarm)	Enroute/ On-Scene	BAS	All	
Location of each detector in alarm within building (on building outline for enroute, on floor plan for on-scene) and what it is (e.g., fire, intrusion, hazardous materials).	Enroute/ On-Scene	BAS/ BIM	All	
Building occupancy (abandoned, vacant, number of young children, high occupancy, number of elderly). Estimates should be based on time of day.	Enroute/ On-Scene	BIM/ FD	All	"FD" indicates this will be updated by fire department during regular inspections.
Building condition (let burn, unsafe to enter, dangerous roof, sprinklered and other suppression systems).	Enroute/ On-Scene	BIM/ FD	All	
Building type (single family, commercial, gas storage, school)	Enroute/ On-Scene	BIM	All	
Building style (one story, two story, n story, auditorium, sublevels, etc) include square feet	Enroute/ On-Scene	BIM	All	
Building construction (type I, II, III, IV or V; fire resistive, non-combustible or limited combustible, ordinary, heavy timber/ wood frame)	Enroute/ On-Scene	BIM	Fire	
Roof construction (light weight metal or wood trusses)	Enroute/ On-Scene	BIM	Fire	
Hazards—location and identification of unusual hazards (above ground propane tank, gas lines, chemicals, etc)	Enroute/ On-Scene	BIM/ FD	All	
Location of fire hydrants on map with building outline. Nonstandard thread sizes should be noted with the hydrant	Enroute	City	Fire	
Location of fire department hookups for sprinkler system/standpipes	Enroute	BIM	Fire	
Other sources of water nearby	Enroute	City	Fire	
Location of vehicle staging areas and entrances and exits to building	Enroute	BIM/ FD	All	
Police on the scene	Enroute	Dispatch	All	Indicating scene is secure
Shots fired (indicating police presence required)	Enroute	Dispatch	All	From 911calls or police on scene.
Location of obstacles to vehicles such as narrow streets , overhead clearances and elevation changes	Enroute	City	Fire	
Photos of building	Enroute	City	All	
Fire suppression system type and status (flowing, not)	Enroute/ On-Scene	BAS	Fire	

Table 2 Required on-scene information elements (to be shown in on-scene display)

Information element	When needed	Data Source	Service	Notes
Location of key box	On-Scene	BIM	All	
Location of doors, windows (with types and which can be used for egress), stairwell risers, fire walls (with ratings and area separation), roof access, fire sensors.	On-Scene	BIM	All	
Location of firefighter equipment, heavy objects on roof	On-Scene	BIM/ FD	Fire	
Location of security sensors, closed circuit TV cameras, occupancy sensors, security control room	On-Scene	BIM	Fire/ police	
Location of fire alarm panel and remote annunciator panels	On-Scene	BIM	Fire	
Location of utility shutoffs	On-Scene	BIM	Fire/ police	
Location of master sprinkler shutoff	On-Scene	BIM	Fire	
Location of building generator (with indication of what it powers)	On-Scene	BIM	Fire/ police	
Location of building system controls (HVAC, smoke control, others), areas covered, and indication of which ones should and should not be used by the responders	On-Scene	BIM	Fire	
Location of areas of refuge within building	On-Scene	BIM	All	
Location of elevators (note if evacuation quality), with floors served, and location of elevator overrides and how to control it.	On-Scene	BIM	All	
Elevator status: floor and direction, presence of smoke in elevator or shaft, presence of heating in controller.	On-Scene	BAS	All	
Location of convenience stairs/evacuation stairs	On-Scene	BIM	All	
Location of sprinklers and other fire suppression systems	On-Scene	BIM	Fire	
Potential building hazards that may require decontamination	On-Scene	BIM/ FD	All	
Location of extremely valuable materials	On-Scene	BIM/ FD	Fire/ police	
Location of vertical openings	On-Scene	BIM	Fire	
Contact number for building engineer	On-Scene	BIM	All	
Presence and location of persons with special needs	On-Scene	BIM/ BAS/ dispatch	All	May be fixed information, reported by BAS, or called in
Locations of fire detectors, security sensors/stations, CBR and other sensors in alarm.	On-Scene	BAS	All	
Location and condition of smoke	On-Scene	BAS/ DSS	All	Requires intelligent analysis
Presence of smoke in elevator shafts or stairwells	On-Scene	BAS	All	
Location or area where sprinklers are flowing	On-scene	BAS	Fire	
Local weather conditions (wind, rain, temperatures)	On-Scene	Dispatch/ BAS	All	

Table 3 Required on-scene information (to be shown in plot-plan display)

Information element	When needed	Data Source	Service	Notes
Names and phone numbers of building owners and managers	On-Scene	BIM	All	
Names and phone numbers of utility contact people	On-Scene	BIM	All	
Location of responding units (fire, police, and EMS), on-scene, or enroute	On-Scene	City/ Dispatch	All	
Location of underground pipelines and other utilities	On-Scene	City	Fire/ police	
Indicated water (foam, other) runoff or water table (flooding) problems	On-Scene	City/FD	Fire	
Evacuation routes (streets)	On-Scene	BIM	All	
Location of triage or evacuation area	On-Scene	IC	All	
Outdoor chemical/radiation staging area(s)	On-Scene	IC or BIM/FD	All	
Hazmat response special equipment requirements	On-Scene	City/BIM/FD	Fire	Online database that gives required response to a given CBR situation (entered by IC)
Hospital availability	On-Scene	Dispatch	EMS	
Helicopter availability	On-Scene	Dispatch	EMS	
Helicopter landing areas	On-Scene	City/FD	All	
Location of police line necessary to isolate the incident	On-Scene	IC	All	May require intelligent system

Table 4 Future information elements

Information element	When needed	Data Source	Service	Notes
Presence (location) of occupants in building	Enroute/ On-Scene	BAS/ dispatch/ DSS	All	From 911 calls, visual sightings, or sensors in building
Routing information for emergency equipment to reach the building in case of construction	Enroute	City	All	
Exposures (other buildings' exposures to fire incident or exposure of responders in case of shooting, etc.)	Enroute/ On-Scene	BAS/City/DSS	All	
History of location in case fire stages before police arrive	Enroute	City	Fire, EMS	
Warnings of structural collapse based on material type, fire location, fire size and duration	On-scene	BAS/DSS	All	Calculated information
Alarm, occupant, and system histories of building	On-scene	BAS	Fire/ police	For tracking fire movement, intruder movement, and for post-incident analysis
Suggested hazard perimeter (e.g., bomb blast radius, chemical fire plumes, and exterior fire spread)	On-Scene	IC/ DSS	All	For crowd control and responder safety—calculated based on knowing the hazard
Display of first responder location, health and equipment status	On scene	Future system	All	
Video feed from security cameras in building or from first responder mounted cameras	On scene	BAS	All	
Predicted smoke (chemical, biological, radioactive/ CBR) plume	On-Scene	City/ DSS	All	
Confidence in the incident being real (based on calculated fire size)	Enroute	BAS/DSS	All	Requires intelligent software to analyze fire system data
Location and extent of CBR contamination in buildings	On-scene	BAS/DSS	All	

Information elements organized by data source

The information elements of Tables 1-3 are re-organized below according to the first listed data source in Tables 1-3.

Dispatch

1. Police on the scene
2. Shots fired (indicating police presence required)
3. Local weather conditions (wind, rain, temperatures)
4. Hospital availability
5. Helicopter availability
6. Location of responding units (fire, police, and EMS), on-scene, or enroute

Municipal data (city)

1. Map of area (plot plan) showing location of the building, street names
2. Name and address of building (also in BIM)
3. Location of fire hydrants on map with building outline. Nonstandard thread sizes should be noted with the hydrant
4. Location of obstacles to vehicles such as narrow streets , overhead clearances and elevation changes
5. Location of underground pipelines and other utilities
6. Indicated water (foam, other) runoff or water table (flooding) problems
7. Evacuation routes (streets)
8. Helicopter landing areas

BIM (Building Information Model)

1. (/FD) Building occupancy (abandoned, vacant, number of young children, high occupancy, and number of elderly). Estimates should be based on time of day.
2. (/FD) Building condition (let burn, unsafe to enter, dangerous roof, sprinklered and other suppression systems).
3. (/FD) Hazards—location and identification of unusual hazards (above ground propane tank, gas lines, chemicals, etc)
4. (/FD) Location of vehicle staging areas and entrances and exits to building
5. (/FD) Location of firefighter equipment, heavy objects on roof
6. (/FD) Potential building hazards that may require decontamination
7. (/FD) Hazmat response special equipment requirements
8. (/FD) Location of extremely valuable materials
9. Photos of building
10. Building type (single family, commercial, gas storage, school)
11. Building style (one story, two story, n story, auditorium, sublevels, etc) include square feet
12. Building construction (type I, II, III, IV or V; fire resistive, noncombustible or limited combustible, ordinary, heavy timber or wood frame)
13. Roof construction (light weight metal or wood trusses)
14. Location of key box
15. Location of doors, windows (with types and which can be used for egress), stairwell risers, fire walls (with ratings and area separation), roof access, fire sensors
16. Location of security sensors, closed circuit TV cameras, occupancy sensors, security control room
17. Location of fire alarm panel and remote annunciator panels
18. Location of utility shutoffs

19. Location of master sprinkler shutoff
20. Location of building generator (with indication of what it powers)
21. Location of building system controls (HVAC, smoke control, others), areas covered, and indication of which ones should and should not be used by the responders
22. Location of areas of refuge within building
23. Location of elevators (note if evacuation quality), with floors served, and location of elevator overrides and how to control it.
24. Location of convenience stairs/ evacuation stairs
25. Location of sprinklers and other fire suppression systems
26. Location of vertical openings
27. Contact number for building engineer
28. Presence and location of persons with special needs
29. Names and phone numbers of building owners and managers
30. Names and phone numbers of utility contact people

BAS (Building Automation System)

1. Identification of type of alarm: fire, security, CBR (chemical, biological, radiation), other. List all classes of alarms present.
2. (/DSS) Confidence of incident being real (based on number of sensors in alarm)
3. Location of each detector in alarm within building (on building outline for enroute, on floor plan for on-scene) and what it is (e.g., fire, intrusion, hazardous materials).
4. Fire suppression system type and status (flowing, not)
5. Elevator status: floor and direction, presence of smoke in elevator or shaft, presence of heating in controller.
6. Locations of fire detectors, security sensors/stations, CBR and other sensors in alarm.
7. (/DSS) Location and condition of smoke
8. Presence of smoke in stairwells
9. Location or area where sprinklers are flowing

IC

1. Location of triage or evacuation area
2. Outdoor chemical/biological/radiation staging area(s)
3. Location of police line necessary to isolate the incident

Section II Interface Design for Building Incident Response

As part of our work to define a set of building incident information for first responders and to develop the technology for moving that information from building to first responder, we have needed to address the issue of how to present the information in a display. We consider our recommendation here as preliminary, and know that there will be many different applications that might present all or parts of this information in different ways. As part of our ongoing work on this project, we will continue to address the display issue with two more small workshops that will allow first responders to interact with our building incident tactical information demonstration in order to get more feedback on this presentation issue. Perhaps there are some concerns that NEMA has that could be addressed simultaneously as part of these workshops.

Two displays are envisioned. The purpose of these displays is to provide timely access to critical information required to mitigate fire and other incidents in building scenarios. The displays could be located on the fire apparatus, at dispatch, and in the building command/control center. Both displays would be used by the incident commander to help manage the fire (or other) incident. Other personnel would use these displays as guides to understand the incident.

The first display (Plot-plan/ Enroute) is a view of the building footprint in a GIS type application where the building is seen with respect to surrounding streets and buildings. This is the view needed enroute to the incident and provides information for staging at the building incident, but it is also needed after arrival on-scene. We present here our understanding of what the layout might look like for this view (plot-plan) and what information relative to a building incident should be presented.

The second display (On Scene/ Building), used primarily at the incident site and dispatch, would provide detailed event information for the building incident. This is envisioned now as a floor plan display, showing the incident floor with icons indicating events that are occurring in real time, as well as all the building configuration information needed by first responders. Views of all floors in the building would be accessible from this display. This display presents more information about the incident and would be the primary interface used by the incident commander when at the scene.

Plot-plan Display

- Address Text Field – Name and address of building
- Static Building Information Field – Building type, style, condition, occupancy, construction and roof construction. Example: Commercial, 3 story & basement, Sprinklered, 40, III, metal truss.
- Dynamic Building Information Field – Confidence in alarm, location of alarm (floor), sprinklers flowing, CBR sensors in alarm, alarm duration. Example: High, third floor, sprinkler yes, R sensor, 2 minutes.
- Staging Field – stage yes or no, shots fired, police on scene. Example: Stage yes, Shots no, Police yes.
- Plot Plan should be resizable – building outline with fire hydrants, building hookups, access points, staging areas, egress areas, unusual building hazards and location of nearby water sources.
- Plot Plan should provide local street information including street closures for construction.

- In the city block view, the building with the fire should be highlighted and buildings that are smart buildings designated.
- Zoom control should be accomplished by touch screen with three choices – zoom in, zoom out, reset to city block size. Zooming will preserve the center screen location.
- Navigation control should be accomplished by touch screen with up/down side to side control.
- Next Screen Control is a touch control that toggles between the Enroute Screen and the Fire Ground Screen.

<table>
<tr><td colspan="2">Address Text Field</td></tr>
<tr><td colspan="2">Static Building Information Field</td></tr>
<tr><td colspan="2">Dynamic Building Information Field</td></tr>
<tr><td colspan="2">Staging Field</td></tr>
<tr><td>Zoom Control</td><td rowspan="3">Plot Plan</td></tr>
<tr><td>Navigate Control</td></tr>
<tr><td>Next Screen Control</td></tr>
</table>

On-Scene Display

- Address Text Field – Name and address of building
- Static Building Information Field – Building type, style, condition, occupancy, construction and roof construction. Example: Commercial, 3 story & basement, Sprinklered, 40, III, metal truss.
- Dynamic Building Information Field – Confidence in alarm, location of alarm (floor), sprinklers flowing, CBR sensors in alarm, alarm duration. Example: High, third floor, sprinkler yes, R sensor, 2 minutes.
- Staging Field – stage yes or no, shots fired, police on scene. Example: Stage yes, Shots no, Police yes.
- Building Display Field – Simplified floor plan showing locations of rooms, doors, and stairways. Included in the display would be the location and type of activated detectors. The location of hot smoke and suspected fires would be displayed by coloring suspected region, red for fire, orange for hot smoke and green for smoke. Icons would be used for radiation, chemical or biological hazards.
- Information Field – Display for specific information associated with an Information Control Button.
- Zoom control should be accomplished by touch screen with three choices – zoom in, zoom out, reset to building size. Zooming will preserve the center screen location.
- Navigation control should be accomplished by touch screen with up/down side to side control.

- Next Screen Control is a touch control that toggles between the Enroute Screen and the On-Scene Screen.
- Information Control Button – Used to overlay icons on the Building Display Field. Icons would be used to represent CBR sensor alarms, security alarms, location of standpipes and stored firefighter hear, firewall ratings, location of hazardous materials with indication of hazard type, Utility shutoffs, fire panels, elevator condition, location of valuable assets, contact numbers for building engineers and owners.
- Event List – running field of events associated with fire and security sensors, sprinklers, and elevator operation.

Future Information

- Dynamic Building Information Field – Fire size, water required, potential for collapse.
- Building Display Field - visibility, location of flowing sprinklers, CBR hazard levels, location of occupants in building, location of firefighters.

<table>
<tr><td rowspan="4">Information Control</td><td>Address Text Field</td></tr>
<tr><td>Static Building Information Field</td></tr>
<tr><td>Dynamic Building Information Field</td></tr>
<tr><td>Staging Field</td></tr>
<tr><td>Event List</td><td rowspan="2">Building Display Field</td></tr>
<tr><td>Zoom Control</td></tr>
<tr><td>Navigate Control</td><td rowspan="2">Information Field</td></tr>
<tr><td>Next Screen Control</td></tr>
</table>

We have included (below, next page) a display that we used in the demo. It does not include all the necessary features but does represent the limitations that are faced designing displays.

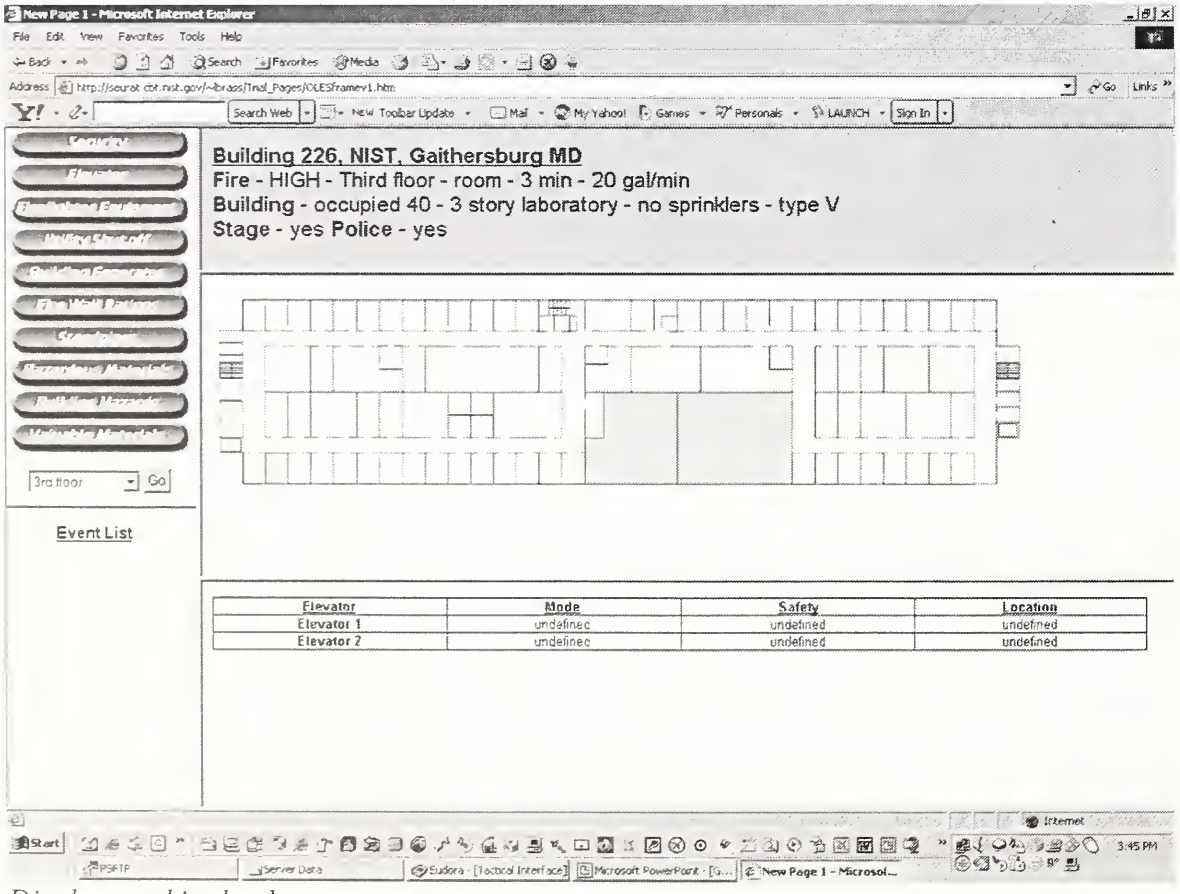
User Interaction with Displays

Displays used on mobile units will be operated either by touch screen or by function keys, although voice-activated displays are also a possibility. Mouse and keyboard interactions will be restricted to use at dispatch or in command vans. For displays on mobile units we recommend the following characteristics:

- Operated by touch screen or function key
- Zooming will preserve the location of the center of the screen
- A touch screen or function key will reset the view to a full floor view
- A touch screen or function key will move the view to the initial incident floor and center on the location of the first alarm
- A touch screen or function key will allow the user to move from floor to floor
- A touch screen or function key will toggle between en-route and on-scene screens

Displays used at dispatch and in command vans will have the following characteristics:

- Can be operated by touch screen, function key, mouse and be menu driven.
- Zooming will preserve the location of the center of the screen
- A single action will:
    1. reset the view to the full floor
    2. move from floor to floor
    3. change the location on a floor
    4. apply overlays of information to the screen
    5. pull down menu items
    6. toggle between enroute and on-scene displays



Display used in the demo.

Appendix C NIST Experimental Implementation Report

Introduction

As part of the deliverables for this project, BFRL researchers demonstrated a method for moving building data from a building out to a user interface in the hands of a first responder. This demonstration involved a simulated building emergency where an intruder enters one of the NIST laboratory buildings after-hours, breaks into a lab, and proceeds to set a fire. The fire was modeled and simulated data from the fire, as well as simulated access control sensor signals were sent to a building information server. A graphical user interface in the hands of first responders was used to subscribe to the building server and download real-time data from the information server as the simulated incident progressed. A schematic of the various elements of the data path from building to user client are shown in Figure 1.

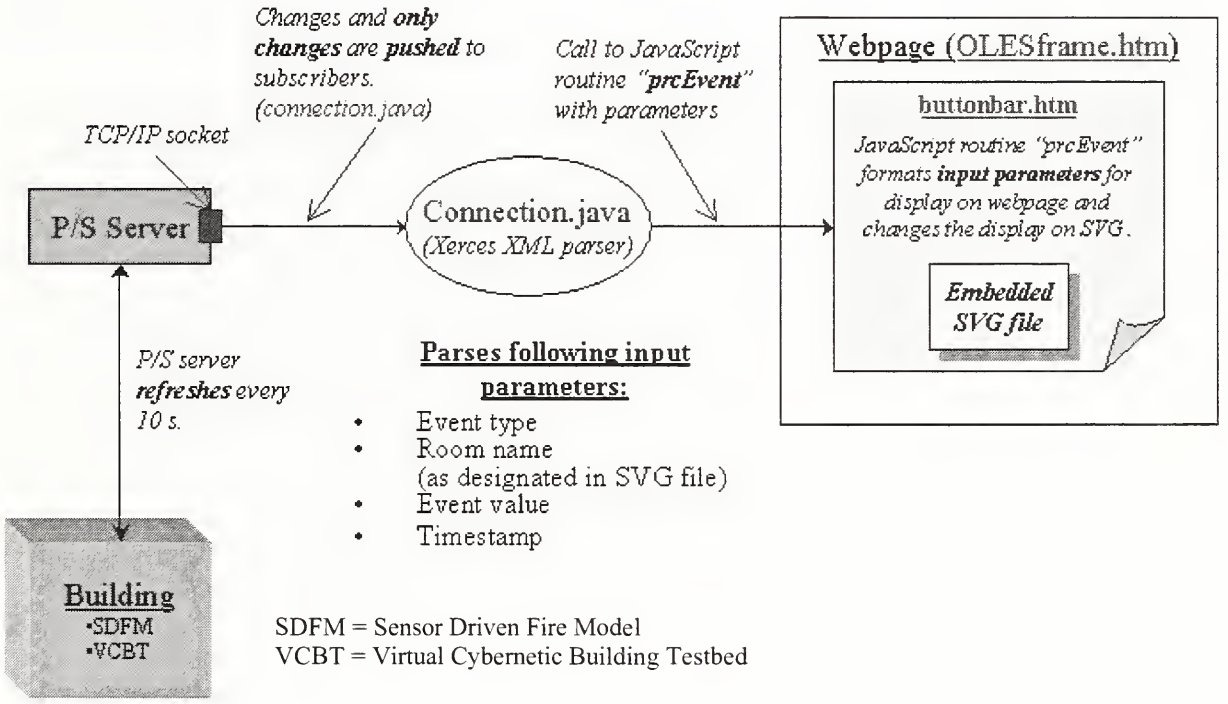


Figure 2 Schematic of data path from building to user interface.

The goal of this work has been to identify the information available from building control systems that would be of use to emergency responders, to identify a means to get the information from the building to the emergency responder, and then to work toward standardization of that data path. One of the deliverables of the project was to demonstrate the flow of data from a building to a first responder's graphical user interface (GUI). This report documents the experimental implementation work that has been done.

The experimental implementation of the building information transfer technology was demonstrated to NIST fire and security personnel in February 2005. The February demonstration involved multiple tasks: selecting a building (NIST Bldg. 226), developing a building incident scenario involving police and fire response to Bldg. 226, developing the input files to a fire model

and running the fire model in order to get accurate fire and smoke development data for the scenario incident, designing a GUI based on input from first responders at our earlier workshop, implementing a graphical floorplan representation of Bldg. 226 in the GUI, developing an XML schema for moving building sensor data of interest from the building control system to the GUI, developing software to encode data into that schema and software (client) to parse the schema and transfer data to the graphical display, and implementation of a publish/subscribe (P/S) server to transfer data from the building to the receiving client. All of these steps will be discussed in more detail below.

For the purpose of communicating the results of our work and potential of the technology, the entire data path, including the building data generated for the emergency scenario, the P/S server and the GUI, was placed on a single laptop, allowing for a portable presentation. This demonstration was presented to NIST fire and security personnel and a short video was created of the demonstration to better communicate the scenario presented on the GUI, and in fulfillment of our deliverable requirement to produce a video of the demonstration. This report provides the details of the demonstration and satisfies in part the second deliverable for a report documenting proposed standards.

Building incident scenario

In preparation for the demonstration, a building and an incident scenario had to be chosen. The Building Research building 226 on the NIST campus was chosen for several reasons. First floor plans were available in electronic format. Second, the floorplan fit satisfactorily with the kind of scenario under consideration. Third, as a real building on the NIST campus, it could be used in a real response to the virtual incident, i.e., the NIST fire and rescue and police could use the GUI to inform their response to the virtual incident as if it were a real incident. The goal of a real response to a virtual incident is to: demonstrate to emergency responders the potential for the technology to aid response; to have feedback from responders on the performance of the technology; and finally to allow us to put together a video in fulfillment of project commitments.

The scenario was designed with two goals in mind. The first goal was to involve both police and fire in the response. In fact, most fire emergencies involve police response in order to help with security and traffic outside the building. However, a scenario that begins with an intrusion followed by arson was chosen. Thus the police arrive first to investigate the intrusion and the scene quickly changes to a fire scene. The second goal was to highlight as many building control systems as was reasonable. The final scenario begins with an intrusion alert from the access control system, followed by more alerts from door and motion sensors. The elevator system reports motion of an intruder going up to the third floor. The fire system reports temperature and smoke conditions.

Technical Components Implemented in Demonstration

Publish Subscribe (P/S) server

The publish and subscribe server is the mechanism used to deliver messages from a building to a person who needs information about that building. For the purposes of the demonstration, a publicly available server implementation was chosen—the Unity server, which is just one of several implementations of publish and subscribe technology. Publish and subscribe technology organizes data into *topics*; for example, in online chat applications an individual can subscribe to all the conversation in a chat room dedicated to a certain topic. The Unity server likewise refers to topics as rooms. In a full building-to-first responder system, one could envision dividing the

types of information from the building into different topics: a building could be divided topologically by floor or by building systems/functions or by the needs of different types of users. In this demo all building information was grouped into a single topic ("Bldg. 226") such that all building data was published to this one topic and the receiving client (GUI) subscribed to this one topic.

When messages are published to the server a message router is needed to deliver the message to the correct topic(s). In this demo all messages were delivered to the single Building 226 topic. If more than one topic were required then the destination(s) of the message should be able to be determined by the contents of the message. After the routing and retention of messages the server relays the messages to the topic subscribers. In the case of the demo, the only subscriber was the receiving user's GUI.

An added feature that was implemented was the retention of messages that had been published about the building. This was done so users could get all of the relevant information about the building that was published before the user subscribed to get building information. An administrative panel was also developed to view the messages being held by the server and to allow messages to be removed from the server.

The Virtual Cybernetic Building Testbed (VCBT)

The VCBT combines computer simulations, real BACnet enabled HVAC controllers, and environmental data to emulate a building in the laboratory. The VCBT also includes a BACnet enabled fire panel connected to smoke and heat detectors, and the virtual building is being expanded to include real access control and lighting systems. During emulation tests, data from the computer models are transmitted to the inputs on the HVAC controllers, simulating the data they would receive in a real building. The output signals from the controllers are then returned to the computer models. The models calculate the effects of the controller actions on the building environment, and generate the next set of input data for the controllers. This completes one cycle of the VCBT, with a new cycle starting every 10 seconds. The use of measured environmental data allows the VCBT to model conditions in heating, cooling, or swing seasons.

The VCBT contains computer simulations which model the entire building, except for the HVAC controllers, and also contains models which only analyze the data from the other models. These models include the Sensor Driven Fire Model (SDFM) which provides 'best guess' information on the current fire and smoke conditions in each room of the VCBT, based solely on the information sent from heat and smoke sensors.

Data Transfer From the VCBT to the P/S server

Data transferred from the VCBT to the P/S server comes from either simulations in the VCBT using the Sensor Driven Fire Model (SDFM), or from the DataServer program. The output of the SDFM is the condition in each room (i.e., no alarm, possible hazard, low visibility, toxic/thermal hazard, or flashover) represented as a number from 1 to 5.

The DataServer program can emulate the output of the SDFM, as well as send several other data elements, most of which are not generated by any model: smoke control activity in a zone, motion sensor status, door status, access point status, heat sensor status, elevator status, elevator level, elevator occupancy, Fire/EMS staging status, police present or not, and water required to fight the fire. The DataServer provides the option of sending events manually or as directed from a settings file.

The data from the VCBT and the DataServer are sent in an XML format created to efficiently represent data from the VCBT. The VCBT Center and the DataServer communicate with the P/S Server via a standard socket connection.

A new XML schema was designed for data transfer and storage at the P/S Server. The criteria used to guide the development of this schema were that it should be efficient, capable of conveying any one of multiple message types, easily and transparently extendable to new message types, and able to contain multiple messages at the P/S Server. The messages sent from the VCBT and the DataServer use the new schema wrapped in additional XML required by the Unity server. The same format is also used to transfer data from the P/S Server to the subscribed GUI clients.

Data-parsing software

Data from different building system controllers are all directed to one centralized location—the publish/subscribe (P/S) server. The model for a P/S server is that a client requests a subscription to a specific "room"* on the server and once this request is granted, any changes that occur in that "room" are immediately sent to all subscribers to that "room". Behind the interactive display a Java applet establishes a connection to the P/S server via a threaded TCP/IP socket. This Java applet, once connected, then subscribes to the appropriate "room" assigned to the building in question on the P/S server. Messages from the building showing any change in status (event message) are received by the P/S server, and are then in turn sent forth to any clients that are connected and have a subscription to the designated "room". Each broadcast message from the P/S server specifies an event that has occurred in the building, and is sent immediately to the interactive display via XML (refer back to Figure 2). The different elements presented in Fig. 1 are discussed in more detail below.

There are several categories of events that are broadcast by the building and then from the P/S server, including but not limited to data from the: Sensor Driven Fire Model (SDFM, which is monitoring sensors to give higher-level intelligent decision support information such as a room's thermal hazard level), security system (i.e., access point status, door status, elevator status and activation of motion sensors) and fire data (i.e., smoke and heat detectors).

The Java applet utilizes the Apache Xerces XML parser to parse the messages received from the server. The parser filters on four key data points: the *event type* (what type of event occurred in the building, e.g., change in heat sensor status or room condition), the *room identification* (where in the building the event occurred), the *event value* (status of the aforementioned event, e.g., room condition has limited visibility), and the *timestamp* of when the event occurred. These data points are then used as input parameters for the JavaScript "preEvent" routine behind the interactive display. The JavaScript routine uses these data points to make the appropriate changes on the display.

---

* P/S servers are often thought of in terms of chat rooms, where a message designated for a certain room is sent to the server, which in turn forwards that message on to anyone with a subscription to that room. For the purposes of this report the word "room" when surround by parentheses is referring to the section of memory on the server dedicated to receive the data from a physical building structure. In all other cases the word room refers to a physical room inside a physical building structure.

Graphical User Interface

The Graphical User Interface (GUI) was designed with several goals in mind. First and foremost is the first responder requirement that the right information be available at the right time and that it be presented clearly and concisely. Secondly, from a technological perspective, the GUI needs to allow for data transfer technology that uses minimum bandwidth, and the GUI should be implemented with open-source technology to minimize cost, reduce hurdles to industry acceptance, and aid rapid development. It should be noted that a user interface was not promised for this project and that our goal is not to produce a marketable product. Rather, we clearly see that the data transfer technology that we are working on must have an interface to the user in order to demonstrate and "sell" the technology to the end users.

Right information, right time, clearly presented

Our May 2004 Information Workshop produced a detailed list of building information desired by first responders in building emergencies. In addition to the information list, we also received input on requirements for information presentation. Once information has been received from the building it needs to be displayed in a manner that is usable by first responders. This requirement encompasses both the idea of getting the *right information at the right time*, as well as presenting it in a *usable format.*

In terms of timing, fire responders have an enroute stage where higher level info is appropriate, and then an on-scene stage where detailed building information needs to be available. In the limited time that responders have to make use of a GUI, only the information desired should be presented and other information should be held until requested. During the alarm and enroute phase of a fire truck's response the fire fighters are doing so much work getting ready that they have little time to note much information. While once on scene a lot more information is needed to assess and attack the fire.

In terms of presenting data in a usable format, the available data must be presented in an intuitive way. Static building configuration data (e.g., fire equipment locations, floor plans, security office location and utility shut-offs) and real-time data (e.g., fire sensors in alarm or elevators in motion) must both be presented as needed in the viewing window of a display. While the static data are easy to manage, dynamic information can be changing very rapidly and can be complex so it is desirable to present the data in a number of ways.

In order to address the needs for different data enroute vs. on-scene, two graphical interfaces were developed. The initial "**enroute**" screen (Fig. 2) shows the footprint of the building and surrounding area. The building is marked with the approximate position of the fire in the building as well as any special hazards. Text in the frame above the map gives the address of the building as well as the size of the fire and the time since the alarm. Roads and fire hydrants and other topographic information of the immediate surroundings are included to help plan the initial staging. This screen is kept simple to provide the incident commander basic information without overwhelming him.

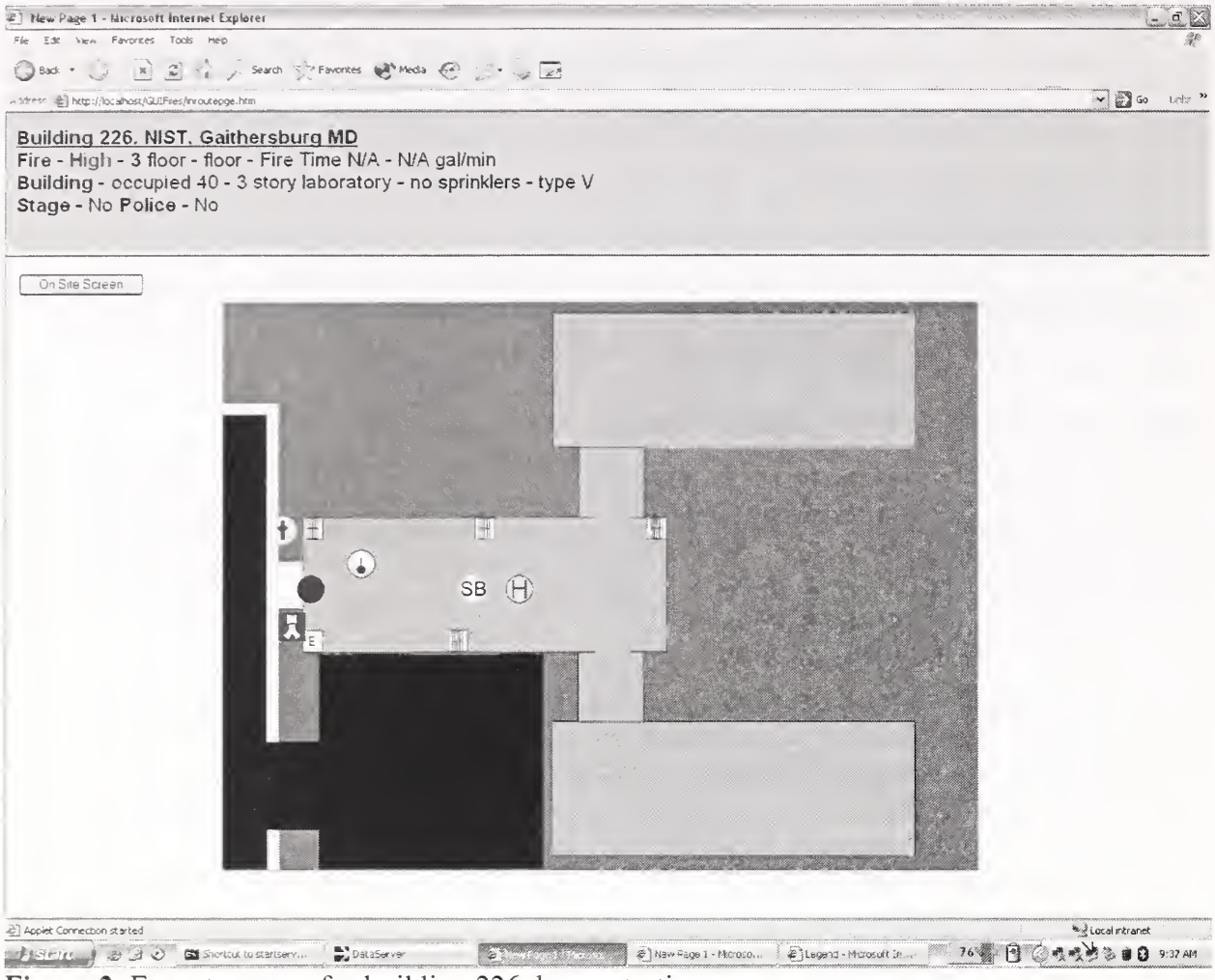


Figure 2 Enroute screen for building 226 demonstration.

On arriving on scene the incident commander presses a button on the "enroute" screen that brings up the "**on-scene**" screen (Fig. 3). The "on-scene" screen has a lot more information available to assist in attacking the fire. The screen is made up of five frames. On the left side at the top is a set of buttons that controls what information is displayed on the floor plan as well as in the details window. Below the buttons is a list of alarms for the incident in chronological order. This event list allows the incident commander to review the history of the incident. Central to the display is the building floorplan, showing the floor selected by the user and displaying information as directed by the user (discussed more below). Above the floorplan is the top frame which presents a fixed set of overview information including static information such as the address, the type of construction, the type of occupancy and the roof type as well as dynamic information such as an estimate of the size of the fire, the amount of water needed to put out the fire and the elapsed time of the incident. The bottom frame is where detailed information is displayed. This could be static information such as the special hazards of the building or where the shut offs for utilities are as well as dynamic information such as the locations and operational modes of the elevators. The details frame can also include a legend for the floor plan that will be discussed next.

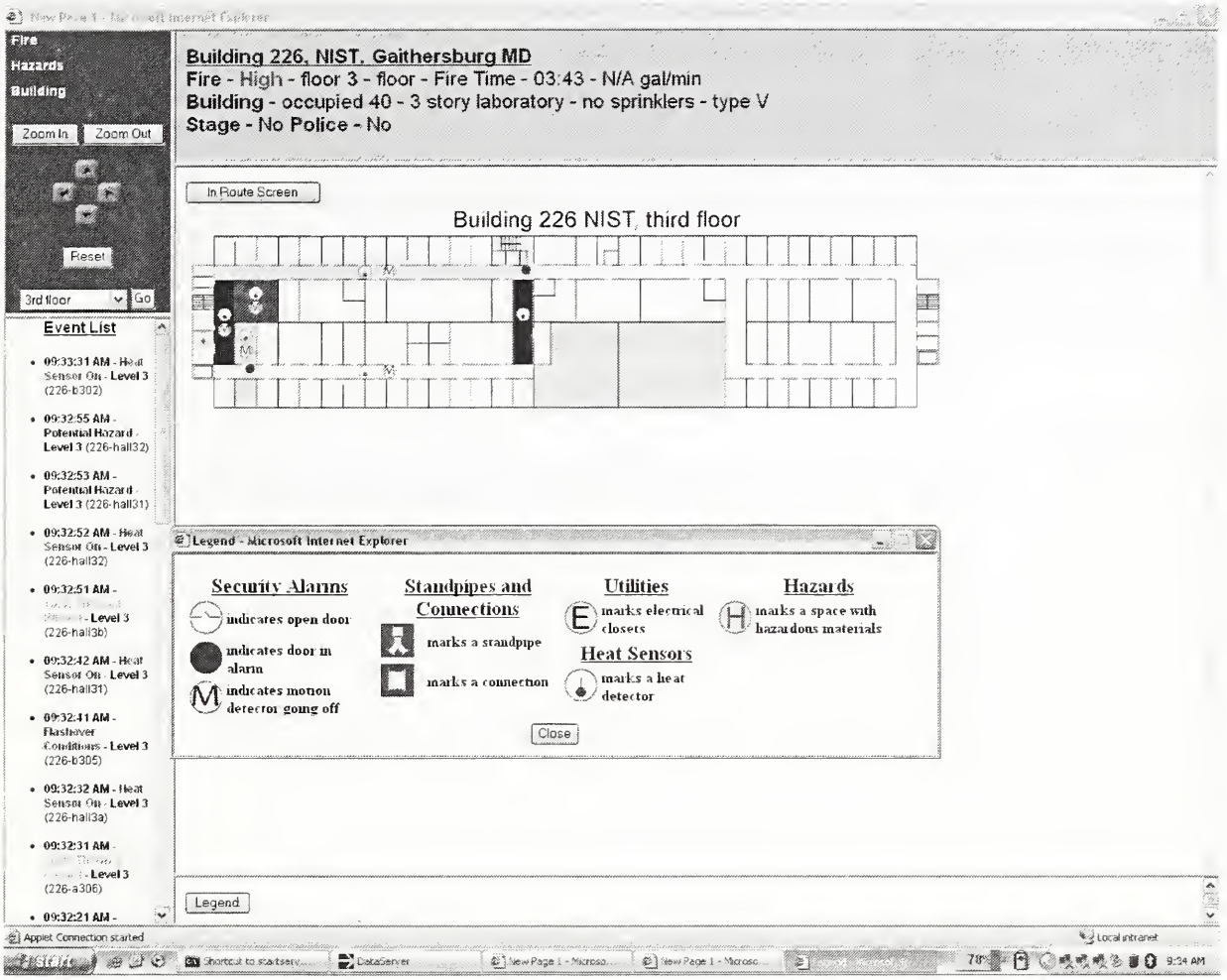


Figure 3 On-site screen for building 226 demonstration.

The center frame is where the floor plan for the building is displayed. Most of the information available is displayed on the floor plan. A single floor can be shown at a time. The buttons on the left determine what information is displayed. When a dynamic event is received from the P/S server (such as a smoke alarm indicating smoke conditions) then the software code generates a symbol in the appropriate position on the floor plan. Then if and when such information is requested, that symbol will be programmatically changed to visible. Static information such as the location of a utility closet or standpipes can be displayed as well as dynamic information. Compartments are color coded to represent the level of hazard in each compartment. White means that the compartment is free of any hazard. Blue indicates that a possible hazard has been detected. Green indicates that a hazard has been detected. Yellow means that there is a significant hazard and that the compartment can only be entered using special equipment. Red means the compartment has flashed over and is lethal to anyone.

Minimum bandwidth, open-source

The goal of design for minimum bandwidth requirements requires that only changes in state (events) are transmitted from the building to the first responder. However, this also requires a database functionality within the GUI where the database maintains the current state. Then when a user requests a data item (say the temperature in a room), the interface simply requests the current value from the database. The publish/subscribe technology does not allow for a request from the client to the building server, but rather the building simply pushes data ("publishes") to the P/S server while the end user's GUI client simply gets updates after subscribing.

The decision to use open-source available technology was made in part to demonstrate the availability of underlying technologies to support this effort. So the displays are built in HTML using JavaScript and Java to support the interactivity and connections with the server. The actual floor plans were implemented using the WWW Consortium's standard for vector graphics, SVG. The advantage of SVG is that it can display not only the information itself, but also can serve as the database for the state of the building. By making use of the group command around a set of icons, the conditions could be set in real time for detectors and compartments but the group could be set to not display. Having a database of the current conditions of the building that can be rapidly updated and quickly accessed is one of the major challenges on the display side.

Conclusion

Details of the technology implemented in the demonstration have been presented. On the day of the demonstration, several NIST fire and police officers had the opportunity to interact with the GUI and see what information might be made available in a real incident, and their response was uniformly enthusiastic. The real response to a virtual incident was helpful in gaining feedback on the interface and thus in the development of the proposal submitted to NEMA. The demonstration itself has been documented on video and is available on CD from the BFRL library, or can be found online (http://www.bfrl.nist.gov/ibr/).

Appendix D Presentation to NFPA 1221 Committee

NIST

Building Information for Emergency Responders

Bill Davis

Fire Research Division

Building and Fire Research Laboratory

Funding: National Institute of Justice,
Department of Homeland Security
NIST Law Enforcement Standards Laboratory

BFRL

NIST

NIST Project Goal

Develop methods and standards to supply information from municipal databases and building systems to public safety officials/first responders in electronic formats during emergency response

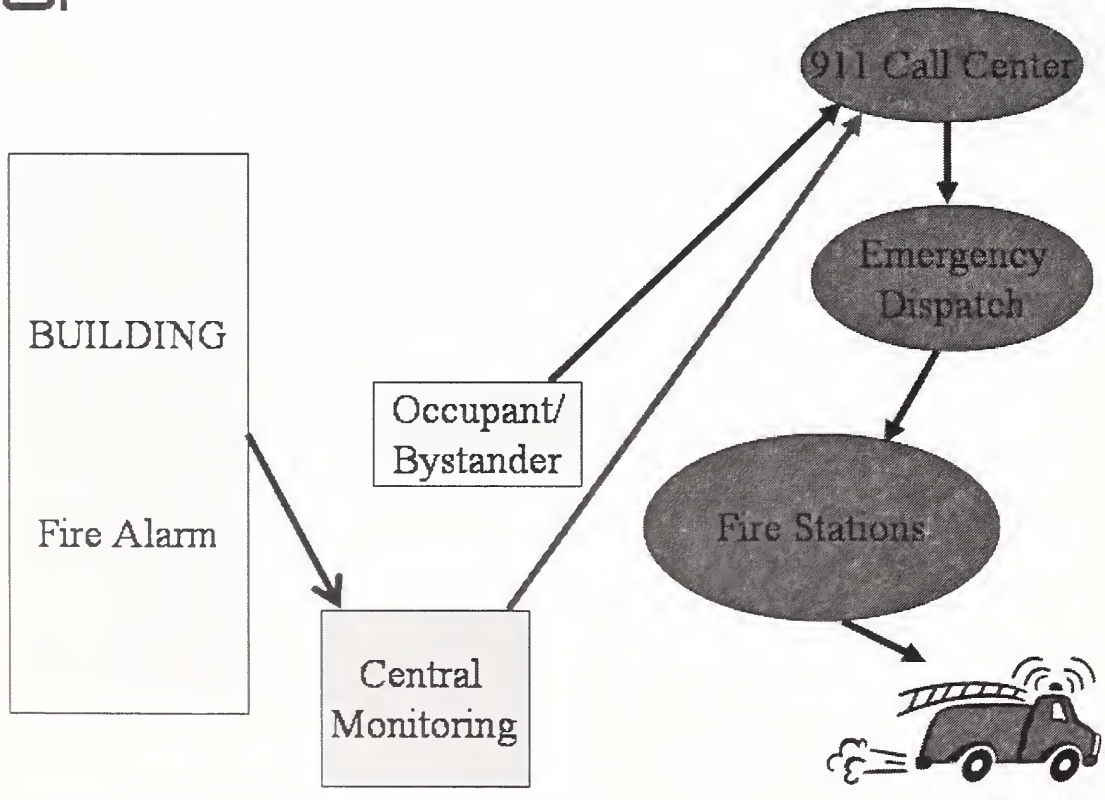
Potential Standards

- Information content
- Representation
- Storage
- Access
- Presentation

Montgomery County Maryland
Emergency Command Center

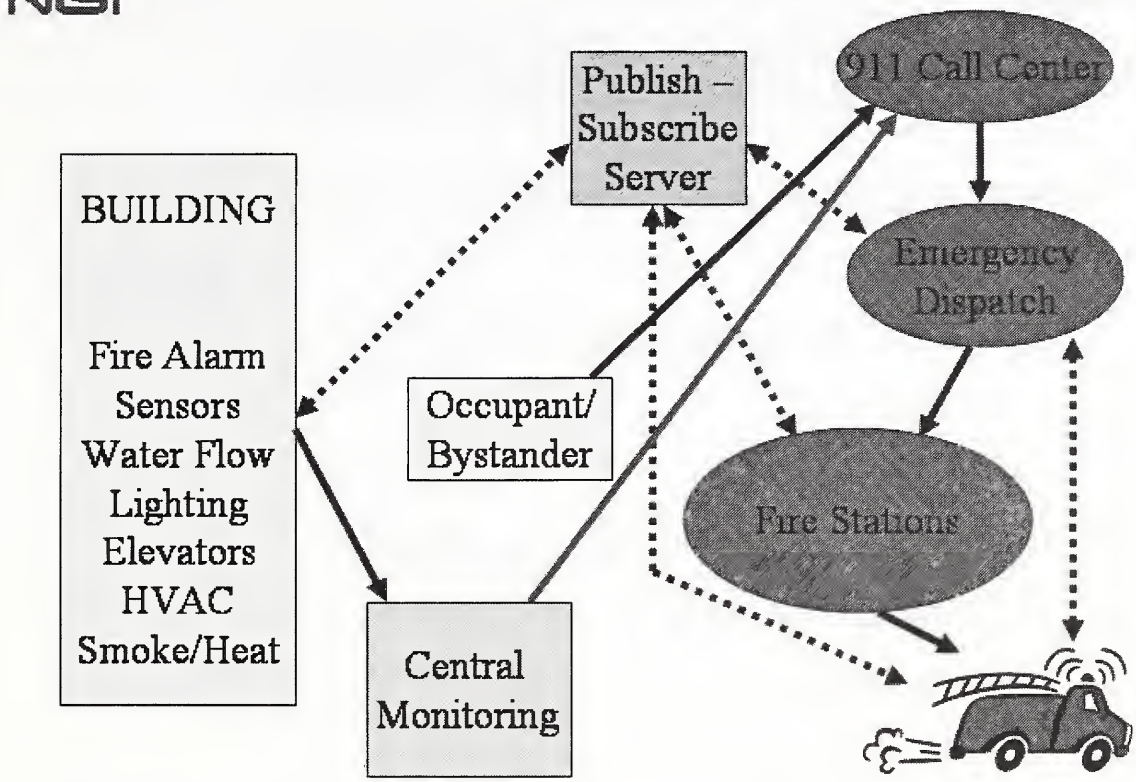
BFRL

NIST



EMERGENCY NOTIFICATION

BFRL



EMERGENCY INFORMATION EXCHANGE

BFRL

Project Status

- **Information Content**
  - Fire Department Preplans
  - Individual Interviews
  - Emergency Responder Workshop, May 2004
  - NFPA Meeting, Salt Lake City, May 2004
  - Workshop Report, NISTIR 7193, 2005

BFRL

NIST

Information Types

- Static (time independent)
  - Preplan
- Dynamic (time dependent)
  - Prevention
  - Mitigation
- Calculated (static/dynamic based)
  - Decision Support
  - Response

BFRL

NIST

Storage and Access

- Municipal Database to a Building Information Model (BIM)
- BIM to a reduced Building Information Model (rBIM)
- Publish/Subscribe Server (P/S)
- XML schemas for information transfer
- Interaction with Global Building Standards such as IFC (Industry Foundation Classes, developed by the International Alliance for Interoperability)

BFRL

NIST

Presentation

- Types of Display Screens
  - Enroute
    - Location and staging
    - Size-up information
    - Hazards
  - Fire Ground/Dispatch
    - Size-up information
    - Static building information
    - Location of fires and smoke
    - Developing hazards
    - Building systems information

BFRL

NIST

NIST Demonstration

- Building simulated using – VCBT (Virtual Cybernetic Building Test-bed)
- Fire simulated using – ZFM (Zone Fire Model, lean version of CFAST)
- Decision support system –SDFM (Sensor-Driven Fire Model)
- Information transfer - Pub/Sub server

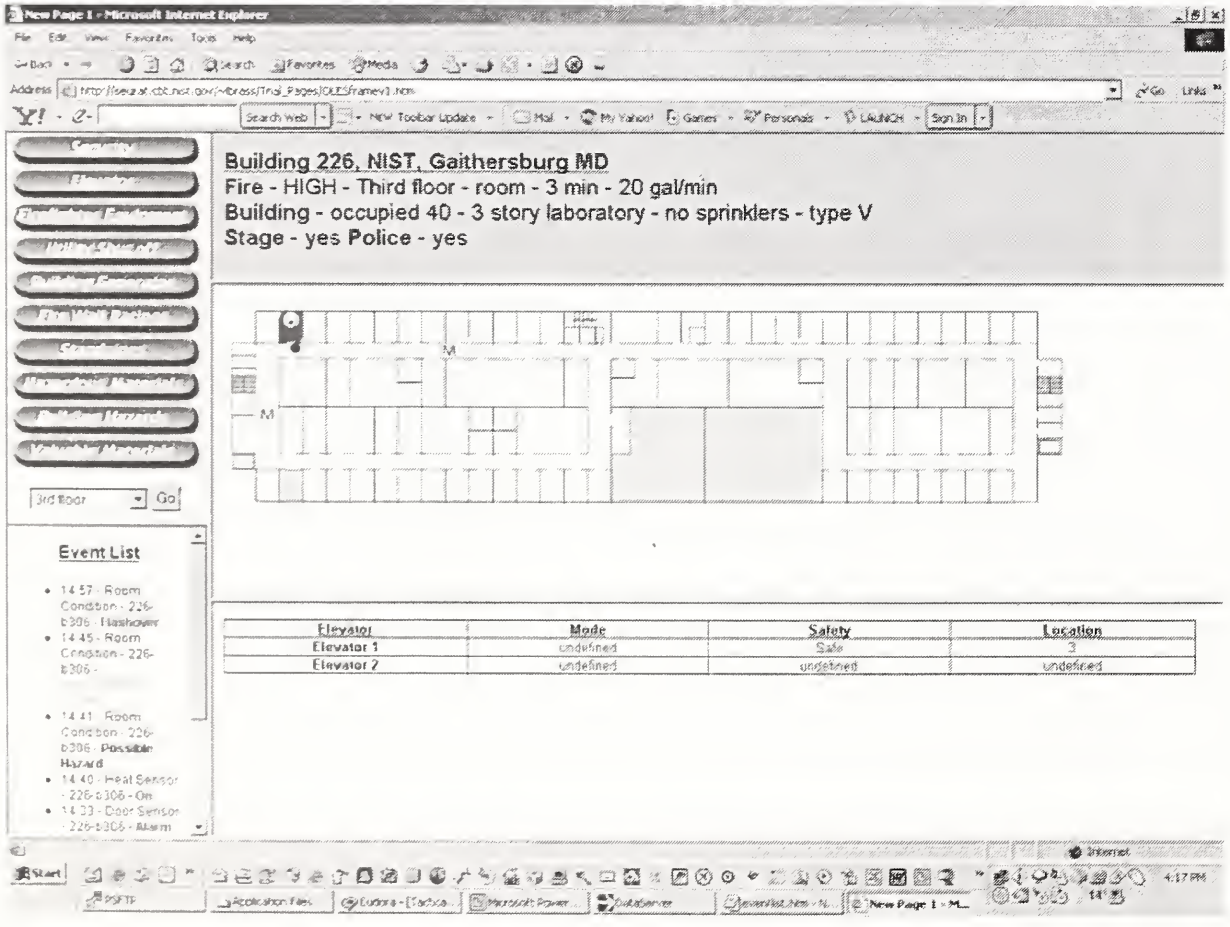
BFRL

NIST

Static Information

- Preplanning
- Training
- Enroute to fire ground

BFRL



NIST

Next Steps

- NIST Demonstration
- Wilson N. C. Demonstration
- Information Standards recommendations submitted to NEMA and subsequently to NFPA
- Emergency Responder Workshops on presentation screens

BFRL

NIST

Project Members

- David Holmberg – Security
- Kent Reed – Pub/Sub server and BIM
- Mike Galler - VCBT
- Steve Treado - Security
- Bill Davis – SDFM, ZFM, and Information Content
- Paul Reneke – Presentation software and ZFM
- Laurie Brassell – Presentation software
- Bob Vettori - Information
- Walter Jones - Consultant
- Dave Evans - Consultant

BFRL